Aker Secure Mail Gateway

Versão 17/10/2011

AKER
www.aker.com.br

Índice

1. Introdução 11
2. Sobre o Aker Control Center 15
Menus 16
2..1. Menu "Opções" 16
2..2. Menu "Janelas" 17
2..3. Menu "Ajuda" 17
Barras de Tarefas 18
Personalizando o Aker Control Center 18
Chaves de Ativação 22
Atualizações 23
Aba Sistema de Atualização: 24
3. O protocolo SMTP 28
Definição 28
Mensagem e Envelope 28
Mail Exchange 30
Funcionamento 30
Erros de Transmissão 31
3..1. Erros Temporários 31
3..2. Erros Permanentes 32
Comandos SMTP 32
4. Conceitos importantes 35
Clientes conhecidos e desconhecidos 35
Autenticação SPF e Sender-ID 35
4..1. Padrão SPF 36
4..2. Sender-ID 37
5. Instalação 40
Requisitos de hardware e software 40
Para a interface gráfica 40
Instalando o Aker Secure Mail Gateway 41
Instalação da Interface Gráfica para Windows 44
6. Configuração 49

© Aker Security Solutions

Configuração 50
Administração de Restrições 50
Gerenciamento de Administradores 51
Mensagens de Notificação 53
6..1. Servidor 59
Aba Limites de Tempo 59
6..2. Aba Recebendo E-mails 61
6..3. Aba Enviando E-mails 63
6..4. Aba Endereços de Escuta 64
6..5. Aba autenticação SMTP 65
6..6. Aba Mensagens mal-sucedidas 66
6..7. Aba Diretória Temporário 67
6..8. Aba Whitelist e Blacklist 68
6..9. Aba Watch Dog 70
SNMP 71
TCP/IP 73
7. Confirmação de E-mail 80
Aliases 80
Associação de domínios 83
Configuração Geral 84
Modo de treinamento 86
Código de proteção anti-bot habilitado (confirmação manual): 86
Adicionar destinatários para a lista automática de endereços autorizados em mensagens enviadas: 87
Receber mensagens de remetentes anônimos: 87
Lista Automática 87
Listas Manuais 88
Mensagem Modelo 90
Visualizador de Quarentena 91
8. Filtragem de conexão 93
Controle de Flood 93
RBLs 94
Sender-ID/SPF 95

© Aker Security Solutions

Servidores, Domínios e Redes 96
9. Filtragem de E-mail 100
Análise de vírus 100
Análise do Remetente/Destinatário 103
Gray Listing 104
Regras Avançadas 106
Whitelist/Blacklist 107
10. Informação do Sistema 109
Fila de Trabalho 109
Status do Sistema 111
11. Logs 114
Configurações de Log 114
Exportações Agendadas 116
Opções de agendamentos 118
Visualizador de logs 119
12. Plugins 128
Aker Antivírus Module 128
Aker Web Content Analyzer 129
Aker Spam Meter 130
13. Políticas 133
Controle de Acesso 133
Categorias de URL 136
Conteúdo do Corpo e Conteúdo do Header 139
13..1. Conteúdo do Corpo 139
13..2. Conteúdo do Header 141
Endereços de Email 142
Filtragem Externa 148
Filtragem de Spam Meter 149
Número Máximo de Mensagens 153
Tamanho Máximo 153
Tipos de Arquivos 155
Whitelist/Blacklist 157
Ordenação de Filtro 158

© Aker Security Solutions

14. Relatórios 160
Configurações de Relatórios 160
15. Repositórios 165
Repositório de Quarentena 165
Repositório de Sistema 168
16. Entidades 174
Arquivos 175
Autenticadores 176
Domínios 177
Lista de Domínio 178
Filtros Externos 179
Lista de E-mails 180
Listas de Expressões Regulares 181
Listas de Palavras-Chave 183
RBLs 184
Redes 185
Servidores 186
17. Interface Gráfica do Usuário 189
Quarentena de Confirmação 190
Quarentena de Filtros 191
Palavras-Chave Aceitas 193
E-mails Autorizados 193
E-mails não Autorizados 195
Opções Gerais 196
18. Cluster 199
Planejando a Instalação 199
Configurando o Cluster do ASMG 200
18..1. Exemplo de configuração 203
Verificando o status do Cluster 205

© Aker Security Solutions

Índice de Figuras

Figura 1. Acesso ao Aker Control Center. 15
Figura 2. Descrição dos itens da Barra de Tarefas. 18
Figura 3. Janela acesso - Dispositivos Remotos. 19
Figura 4. Editar Dispositivos Remotos. 19
Figura 5. Editar Dispositivos Remotos – alteração do ícone de apresentação. 21
Figura 6. Editar Dispositivos Remotos – escolhas dos ícones. 21
Figura 7. Editar Dispositivos Remotos – seleção da cor. 21
Figura 8. Informações sobre a licença de aplicação. 22
Figura 9. Sistema de atualizações ou correção do ASMG. 24
Figura 10. Escolha do arquivo para carregar os dados de configuração. 25
Figura 11. Sistema de atualização – histórico. 26
Figura 12. Mensagem e envelope. 29
Figura 13. Exemplo de consulta pelo nslookup. 30
Figura 14. Instalação do ASMG - fwinst. 42
Figura 15. Instalação do ASMG – mensagem de configuração inicial. 42
Figura 16. Contrato de licença. 42
Figura 17. Configuração de rede. 43
Figura 18. Módulo de configuração para instalação de rede. 43
Figura 19. Mensagem de criação de administrador. 43
Figura 20. Mensagem de aceitação – criação de certificados. 43
Figura 21. Mensagem de instalação completa. 43
Figura 22. Instalação da Interface Gráfica para Windows. 44
Figura 23. Instalação da Interface Gráfica para Windows - contrato. 45
Figura 24. Tipo de instalação - padrão. 45
Figura 25. Mensagem de inicio de instalação. 46
Figura 26. Status de instalação do Aker Control Center. 46
Figura 27. Mensagem de conclusão de instalação. 47
Figura 28. Janela acesso: Configuração do ASMG. 49
Figura 29. Administração de restrições de Endereço IP/Rede. 51
Figura 30. Gerenciamento dos Administradores. 52
Figura 31. Mensagem de notificação – remoção de vírus. 54
Figura 32. Mensagem de notificação – URL's filtradas. 55
Figura 33. Mensagem de notificação – tamanho do arquivo. 56
Figura 34. Mensagem de notificação – tipo de arquivo. 57
Figura 35. Mensagem de notificação – conteúdo. 58
Figura 36. Servidor – limites de tempo. 60
Figura 37. Servidor – recebendo e-mails. 61
Figura 38. Servidor – enviando e-mails. 63
Figura 39. Servidor – endereços de escuta. 65
Figura 40. Servidor – autenticação SMTP. 66

© Aker Security Solutions

Figura 41. Servidor – mensagens mal sucedidas. 67
Figura 42. Servidor – diretório temporário. 68
Figura 43. Servidor – whitelist e blacklist. 69
Figura 44. Servidor – watch dog. 70
Figura 45. Configuração dos paramentros do protocolo SNMP. 71
Figura 46. Aba de acesso: configuração TCP/IP. 73
Figura 47. TCP/IP - DNS. 74
Figura 48. TCP/IP – Interface. 75
Figura 49. Menu suspenso – inserir alias. 76
Figura 50. TCP/IP - Rotas. 77
Figura 51. Aliases associados a senhas. 82
Figura 52. Aliases associados a usuário existente. 83
Figura 53. Associação de domínio. 84
Figura 54. Configuração geral do ASMG. 85
Figura 55. Configuração Modo de treinamento. 86
Figura 56. Lista automática. 88
Figura 56. Lista manual. 89
Figura 58. Mensagem modelo. 90
Figura 59. Visualizador de quarentena. 91
Figura 60. Controle de Flood. 93
Figura 61. Referenciar as listas do tipo RBL. 94
Figura 62. Sender ID/SPF. 95
Figura 63. Lista de endereços autorizados. 96
Figura 64. Lista de endereços não autorizados. 98
Figura 65. Análise de Virus - Entrada. 101
Figura 66. Análise de Virus - Saída. 102
Figura 67. Análise do remente/Análise dos destinatários. 103
Figura 68. Análise do remente/Análise de destinatários. 104
Figura 69. Gray listing. 104
Figura 70. Gray listing – modo de treinamento. 106
Figura 71. Regras avançadas – Pré-regras. 107
Figura 72. Whitelist/Blacklist. 107
Figura 73. Fila de trabalho - recebendo. 109
Figura 74. Fila de trabalho - processando. 110
Figura 75. Fila de trabalho - entregando. 111
Figura 76. Status do sistema. 112
Figura 77. Configurador de log – configurações gerais. 115
Figura 78. Janela de acesso: Exportações agendadas. 116
Figura 79. Exportações agendadas. 117
Figura 80. Opções de agendamentos. 118
Figura 81. Visualizador de log. 119
Figura 82. Filtro de log de mensagens. 121
Figura 83. Visualizador de log - eventos. 122

© Aker Security Solutions

Figura 84. Visualizador de log - eventos. 123
Figura 85. Filtros. 124
Figura 86. Configurações de log – ações das mensagens. 126
Figura 87. Configuração de acesso ao servidor. 129
Figura 88. Aker web content analyzer. 130
Figura 89. Habilitação do Aker Spam Meter. 131
Figura 90. Controle de acesso. 134
Figura 91. Categorias de URL's – entradas. 137
Figura 92. Configuração das categorias de URL's – saída. 138
Figura 93. Janela de confirmação sobre geração de falsos positivos. 138
Figura 94. Conteúdo do corpo – lista de palavras chaves. 140
Figura 95. Conteúdo do header – lista de palavras chaves. 142
Figura 96. Endereços de e-mail – descarte de mensagens nos padrões descritos. 143
Figura 97. Endereços de e-mail – pular para o próximo filtro mensagens que se encaixam no padrão. 144
Figura 98. Endereços de e-mail – domínio dos rementes. 145
Figura 99. Endereços de e-mail – endereço dos remetentes. 146
Figura 100. Endereços de e-mail – endereço dos remetentes (pular para o próximo filtro). 147
Figura 101. Filtragem externar – ações que podem ser executadas pelos filtros externos. 148
Figura 102. Filtragem do Spam Meter. 150
Figura 103. Número máximo de mensagens. 153
Figura 104. Tamanho máximo de mensagens. 154
Figura 105. Entrada – tipos de arquivos. 155
Figura 106. Entrada – whitelist e blacklist. 157
Figura 107. Ordenação de filtro. 158
Figura 108. Configuração de relatórios. 161
Figura 109. Opções de agendamento. 162
Figura 110. Repositório de quarentena. 166
Figura 111. Barra dos botões de operações - Repositório de quarentena. 166
Figura 112. Repositório de quarentena - configurações. 167
Figura 113. Repositório de sistema – Serviço inbound. 169
Figura 114. Repositório de sistema – Serviço engine. 170
Figura 115. Repositório de sistema – Serviço Dispatcher. 171
Figura 116. Repositório de sistema – Wblistd. 171
Figura 117. Configuração das entidades. 175
Figura 118. Configuração dos tipos de arquivos. 176
Figura 119. Adicionar entidades. 177
Figura 120. Configuração de entidades – domínio. 178
Figura 121. Configuração de entidades – lista de domínio. 178
Figura 122. Filtro externo. 179

© Aker Security Solutions

Figura 123. Lista de e-mails.....180
Figura 124. Lista de extressões regulares.....182
Figura 125. Lista de palavras-chave.....183
Figura 126. Entidade tipo RBL.....185
Figura 127. Entidade tipo Rede.....186
Figura 128. Entidade tipo Servidor.....186
Figura 129. Tela de acesso inicial ao ASMG- interface gráfica.....189
Figura 130. Quarentena de confirmação.....190
Figura 131. Quarentena de filtros.....192
Figura 132. Palavras-chave aceitas.....193
Figura 133. E-mails autorizados.....194
Figura 134. E-mails não autorizados.....195
Figura 135. Opções gerais.....196
Figura 136. Exemplo de configuração – topologia da rede.....203

Introdução

1. Introdução

Este é o manual do usuário da versão 2.5 do Aker Secure Mail Gateway. Nos próximos capítulos você aprenderá como configurar esta poderosa ferramenta de proteção e controle de E-mails. Esta introdução tem como objetivo descrever a organização deste manual e tentar tornar sua leitura o mais simples e agradável possível.

Como está disposto este manual.

Este manual está organizado em vários capítulos. Cada capítulo mostrará um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Todos os capítulos começam com uma introdução teórica sobre o tema a ser tratado seguido dos aspectos específicos de configuração do Aker Secure Mail Gateway. Juntamente com esta introdução teórica, alguns módulos possuem exemplos práticos do uso do serviço a ser configurado, em situações hipotéticas, porém, bastante próximas da realidade. Buscamos com isso tornar o entendimento das diversas variáveis de configuração o mais simples possível.

Recomendamos que este manual seja lido pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se for necessário, pode-se usá-lo como fonte de referência (para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se achar facilmente a informação desejada).

Em vários locais deste manual, aparecerá o símbolo seguido de uma frase escrita em letras vermelhas. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes de prosseguir com a leitura do capítulo.

Interface texto vs. Interface Gráfica

O Aker Firewall possui duas interfaces distintas para sua configuração: uma interface gráfica remota e uma interface texto local.

- **A interface gráfica remota**

  A interface gráfica é chamada de remota porque através dela é possível administrar remotamente, via Internet, um Aker Secure Mail Gateway localizado em qualquer parte do mundo. Esta administração é feita através de um canal seguro entre a interface e o produto, utilizando um forte esquema de autenticação e criptografia, de modo a torná-la totalmente segura.

© Aker Security Solutions

A interface gráfica é de uso bastante simples e está disponível para plataformas Windows e Linux.

- **A interface texto local**

  A interface texto é totalmente orientada à linha de comando que roda na máquina onde o firewall está instalado. O seu objetivo básico é possibilitar a automação de tarefas da administração do Aker Secura Mail Gateway (através da criação de *scripts*) e possibilitar uma interação de qualquer *script* escrito pelo administrador.

  Como as duas interfaces tratam das mesmas variáveis, a funcionalidade, os valores e os comentários destas têm validade tanto para interface gráfica quanto para a interface texto. Devido a isso, os tópicos referentes à interface texto normalmente serão curtos e se limitarão a mostrar seu funcionamento. Caso tenha dúvida sobre algum parâmetro, deve-se recorrer à explicação do mesmo no tópico relativo à interface gráfica.

Não é possível o uso simultâneo de dois administradores para um mesmo produto, nem o uso da interface texto local enquanto existir uma interface gráfica remota aberta.

O Aker Secure Mail Gateway

O Aker Secure Mail Gateway (ASMG) é um sistema que reúne diversos programas que se integram com o objetivo de oferecer compatibilidade com os protocolos Simple Mail Transfer Protocol (SMTP) e Enhanced ou Extended Simple Mail Transfer Protocol (ESMTP). Atualmente, estes são os protocolos mais utilizados pela Internet para "promover" a troca de mensagens eletrônicas (e-mails).

Um gateway funciona como intermediário no recebimento de e-mails, desconhecendo os usuários finais (destinatários das mensagens). O mesmo acontece com o ASMG (Aker Secure Mail Gateway), que funciona como um "portão" e é instalado estrategicamente numa posição que possibilite interceptar as mensagens antes que elas alcancem o servidor final de e-mails.

O ASMG pode ser definido como um tipo de firewall de e-mails, ou seja, aquele que identifica e deposita as mensagens conforme suas regras de filtragem. Ele realiza filtragens diversas e sofisticadas sobre os e-mails interceptados, decide sobre como será a entrega ao final da análise das mensagens, podendo repassar a versão original ou modificada do e-mail ao servidor final ou mesmo cancelar a entrega, conforme as regras vigentes.

Quando um e-mail alcança o servidor SMTP de seu domínio, ele é normalmente repassado à caixa de correio de seu destinatário sem que seja feita qualquer análise dos seus dados. Por conseguinte, os usuários acabam recebendo muitas mensagens indesejadas (SPAMs), que além de lotar as caixas de entrada de e-mails, muitas vezes contém anexos contaminados por vírus. Com o uso do ASMG,

os e-mails passam a ser analisados através de filtros customizados, com o objetivo de se identificar as referidas situações indesejáveis.

O produto está disponível em duas interfaces gráficas, variando conforme o público-alvo e o seu objetivo de uso. A primeira, denominada **Interface Gráfica de Administração**, tem a função de configurar todas as funcionalidades do produto e deve ser manipulada somente pelos administradores de rede ou usuários que tenham permissão de administração. Já a segunda, denominada **Interface Gráfica do Usuário,** tem como objetivo a configuração de parâmetros particulares de mensagens dirigidas a cada destinatário pertencente ao(s) domínio(s) administrado(s) pela rede em questão. Cada um deles terá acesso a uma interface para configurar parâmetros como remetentes autorizados, remetentes proibidos, dentre outros.

Para facilitar a consulta deste manual, a instalação e a administração de cada interface serão descritas separadamente. A descrição destas interfaces será dividida em duas grandes seções, uma para cada interface. As subseções representam as diversas janelas que compõem cada interface.

© Aker Security Solutions

Sobre o Aker Control Center

2. Sobre o Aker Control Center

*Visando melhor integração entre as ferramentas e agilidade na operação, a Aker desenvolveu o **Aker Control Center**, ferramenta capaz de agregar em uma mesma interface a administração de várias ferramentas: **Aker Secure Mail Gateway**, **Aker Firewall**, **Aker Secure Roaming**, **Aker Antivírus Module**, **Aker Web Content Analyzer**, entre outros. Com interface altamente fácil de usar e totalmente adaptável torna-se possível agregar as diversas funcionalidades que cada um destes sistemas possui e tirar o máximo proveito de todas as ferramentas em conjunto.*

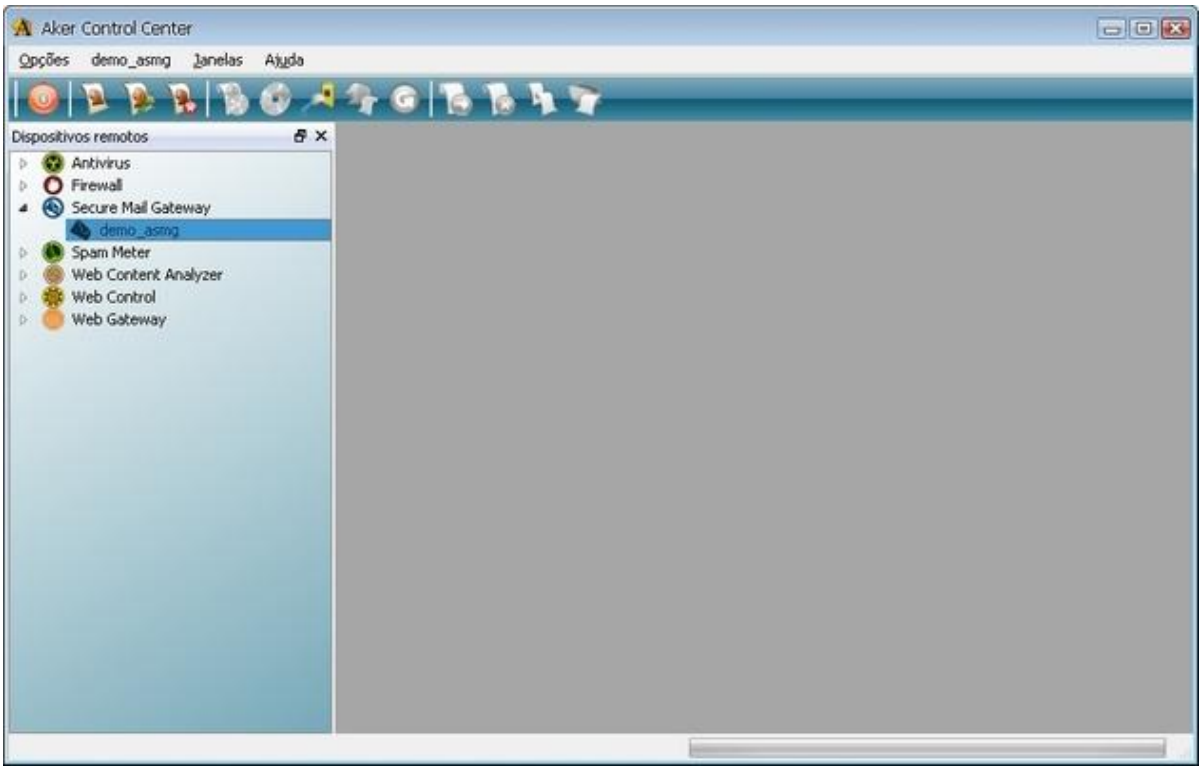

Figura 1. Acesso ao Aker Control Center.

Com o **Aker Control Center** é possivel concentrar vários dispositivos remotos sob a mesma árvore. Ou seja, caso o Administrador gerencie mais de um Gateway de e-mails, por exemplo, poderá inseri-los sob a árvore **"Secure Mail Gateways"** e administrá-los separadamente. A mesma coisa acontece com os outros produtos.

Outra facilidade é que o **Aker Control Center** possibilita a criação de versões de demonstração (demo) de cada uma das ferramentas, podendo configurá-las de maneira independente à versão em produção. O interessante desta função é que o Administrador pode utilizar esta versão de demonstração para ambientar-se melhor com o produto, executar treinamentos e apresentações sem que para isso precise comprometer o serviço que esteja em produção.

© Aker Security Solutions

Outro diferencial a ser destacado é a facilidade em customizar os ícones e cores de cada dispositivo, a fim de diferenciá-los tanto de dispositivos semelhantes quanto de outros dispositivos localizados em locais diferentes na árvore. Com essa identificação visual facilita a administração de vários dispositivos que estejam sob uma mesma árvore.

Este capítulo, explicará todos os menus, botões e formas de customizar **o Aker Control Center**, a fim de que você possa tirar o máximo proveito da ferramenta.

Menus

Os menus estão localizados na parte superior da tela do **Aker Control Center**. Basicamente são três:

- **Opções**, onde podem ser configuradas tarefas gerais;

- **Janelas**, onde podem ser configurar a disposição geral de janelas e barras de tarefas;

- **Ajuda**, onde pode ser encontradas informações de ajuda sobre o **Aker Control Center**.

Adicionalmente, sempre que um módulo for acessado, um menu homônimo a ele estará disponível entre os menus **"Opções"** e **"Janelas"**. Por exemplo, se estiver manipulando um dispositivo de Gateway de E-mails cujo nome é **"Demonstração"**, um menu com este mesmo nome será apresentado na Barra de Menus. Dentro dele, terá opções para edição, deleção e backup das configurações designadas para o dispositivo.

2..1. Menu "Opções"

Tem como função agregar funcionalidades relativas à operação geral do sistema e personalização do ambiente de trabalho. É composto pelos seguintes itens:

- **Textos nos botões:** esta opção define se textos com o nome de cada botão será apresentado abaixo do seu ícone;

- **Show Tooltips:** quando selecionado, mostra exemplos de configuração para aquele dispositivo;

- **Ajuda Rápida:** quando acionado, mostra breve texto de ajuda referente à funcionalidade que está sendo acessada;

- **Mostrar Ícones nos Botões:** dentro da operação do **ASMG**, este botão define se os ícones internos (OK, Cancelar, etc) serão mostrados ou não;

© Aker Security Solutions

- **Tempo de sessão ociosa:** o Administrador pode configurar se deseja ou não terminar uma sessão ociosa após certo intervalo de tempo;

- **Remoção:** mostra mensagem de confirmação de exclusão de itens;

- **Sair:** sai do **Aker Control Center**.

2..2. Menu "Janelas"

Nesta janela podem-se escolher as barras de tarefas e janelas que serão mostradas durante a operação do sistema, além de poder decidir como a tela será organizada. É composto pelas seguintes opções:

Barras de Ferramentas:

- **Sistema:** é a principal barra de ferramentas do **ASMG**;

- **Line Up:** faz com que barras avulsas referentes ao uso de determinadas funções alinhem-se à barra de ferramentas principal;

Janelas: através deste menu é possível selecionar as janelas que estarão disponíveis na área de trabalho. É composto pelas seguintes opções:

- **Ajuda:** carrega a janela que contém informações sobre cada tela acessada;

- **Dispositivos Remotos:** carrega a janela que contém as árvores de dispositivos gerenciados;

- **Entidades:** carrega a janela que mostra todas as entidades referentes a um dispositivo gerenciado;

- **Line Up:** alinha as janelas abertas;

Lado a Lado: organiza as telas de administração lado a lado;

Cascata: organiza as telas de administração em cascata.

2..3. Menu "Ajuda"

Neta janela encontra-se informações gerais sobre o sistema e seus componentes. É composto pelas seguintes opções:

- **O que é isso:** ajuda rápida para a utilização de todos os dispositivos instalados **no Aker Control Center**;

© Aker Security Solutions

• **Sobre:** traz informações gerais a respeito do **Aker Control Center**, com versão de bibliotecas e plugins instalados.

Barras de Tarefas

As Barras de Tarefas agregam diversos botões cuja função é agilizar a realização de tarefas referentes ao uso da ferramenta.

Botão utilizado para sair do Aker Control Center;

Adiciona um novo dispositivo remoto do **ASMG,** Firewall ou Configuration Manager;

Botão que traz as configurações já armazenadas de um determinado dispositivo para edição dos dados;

Exclusão de algum objeto gerenciável administrado pelo Control Center;

Salvar as configurações e alterações dos módulos já criados;

Carregar as configurações de um módulo previamente salvo no Control Center;

Finalizar a conexão com algum módulo administrado pelo Control Center;

Para ter acesso à janela de chave de ativação;

Para ter acesso à janela de atualizações.

Figura 2. Descrição dos itens da Barra de Tarefas.

IMPORTANTE: se estiver utilizand o de demonstração da ferramenta, é necessário clicar no botão **"Salvar"** ao realizar qualquer alteração na configuração atual, a fim de garantir que as novas configurações estejam disponíveis na próxima utilização.

Personalizando o Aker Control Center

Para facilitar a identificação visual de diferentes dispositivos, é possível personalizar os ícones e cores de apresentação dos componentes do Aker Control Center. Desta maneira, o Administrador pode realizar diferentes arranjos dentro da tela, escolhendo uma determinada cor para o mesmo grupo de aplicativos, ou alterando os ícones conforme a região em que o objeto administrado se encontra.

Para realizar a customização, é necessário ter um dispositivo do Secure Mail Gateway cadastrado no Aker Control Center. Para cadastrar um dispositivo:

© Aker Security Solutions

• Se a janela **"Dispositivos Remotos"** não estiver visível, clique no menu **"Janelas"** do Control Center e escolha a opção que possui o nome **"Janelas"**. Marque a opção **"Dispositivos Remotos"**;

Figura 3. Janela acesso - Dispositivos Remotos.

• A seguir, clique com o botão direito do mouse no item **"Secure Mail Gateways"** e escolha a opção **"Novo dispositivo remoto";**

• Preencha os dados requisitados: nome do servidor, endereço IP, usuário e senha. Se preferir apenas usar o modo de demonstração, marque apenas a opção **"Modo de demonstração"** e insira o nome;

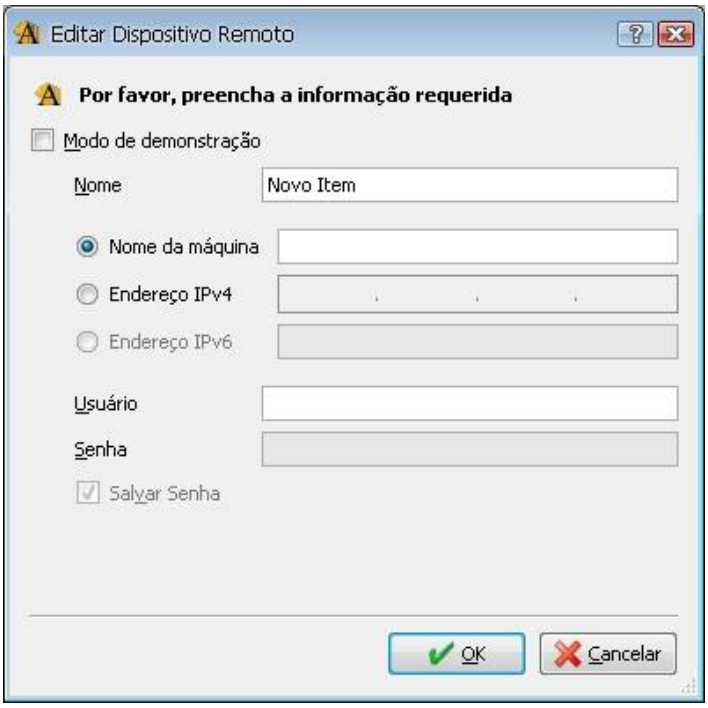

Figura 4. Editar Dispositivos Remotos.

- **Modo de demonstração**: Ao selecionar essa opção será criado um ASMG de demonstração com uma configuração padronizada. Nenhuma conexão real será feita ao tentar se conectar neste ASMG, podendo-se criar quantos ASMG de demonstração for desejado, cada um com a configuração distinta um do outro;
- **Nome**: cadastrar o nome pelo qual o ASMG será referenciado na interface gráfica;
- **Nome da máquina:** Caso o servidor do ASMG o qual se deseja conectar possua um nome associado ao IP da máquina, basta colocar este nome nesta opção para que o Control Center resolva o DNS automaticamente e se conecte no servidor;
- **Endereço**: cadastrar o endereço IP para conectar no ASMG;
- **Usuário**: esse campo identifica o usuário que acessará o ASMG. Este campo grava o usuário, onde aparecerá todas as vezes que o ASMG for acessado.
- **Senha**: a senha do usuário. Caso deixe a caixa *Salvar senha* marcada, não será necessário digitar a senha quando fizer a conexão (a senha aparecerá na tela como vários asteriscos "*"). Caso ela esteja desmarcada, este campo estará desabilitado.

Ao término de preenchimento dos dados, basta clicar em **Ok** e o ASMG estará cadastrado, como o tipo de autenticação selecionado. Caso queira cancelar o cadastro do ASMG, basta clicar em **Cancelar**.

Depois que o dispositivo estiver cadastrado, é permitido alterar seu ícone e cor de apresentação. Para isso, basta clicar com o botão direito do mouse sobre o ícone do dispositivo que você acabou de instalar e clique em **"Editar".** Na janela localize o ícone do dispositivo e clique uma vez sobre ele.

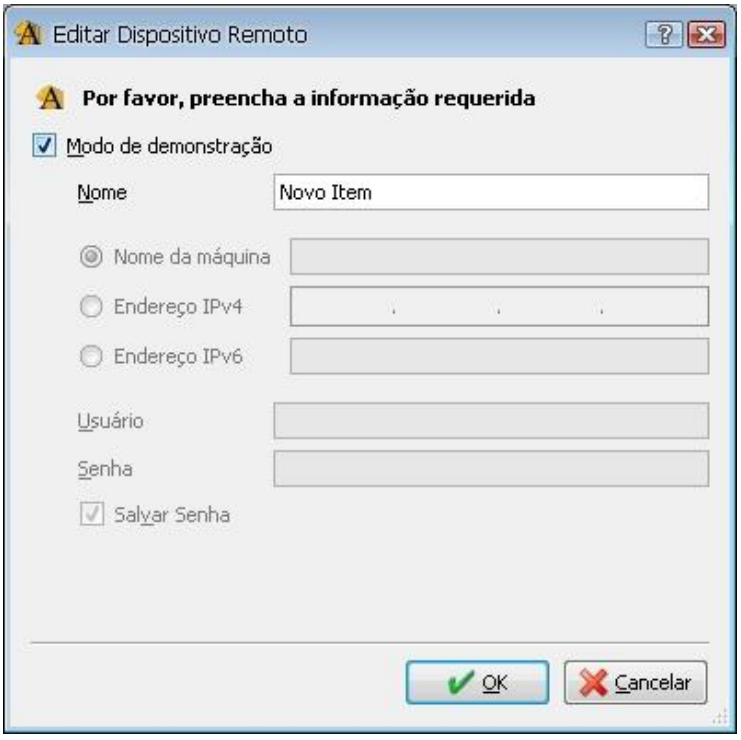

Figura 5. Editar Dispositivos Remotos – alteração do ícone de apresentação.

A nova janela mostra os possíveis ícones que podem ser escolhidos para substituir os já existentes:

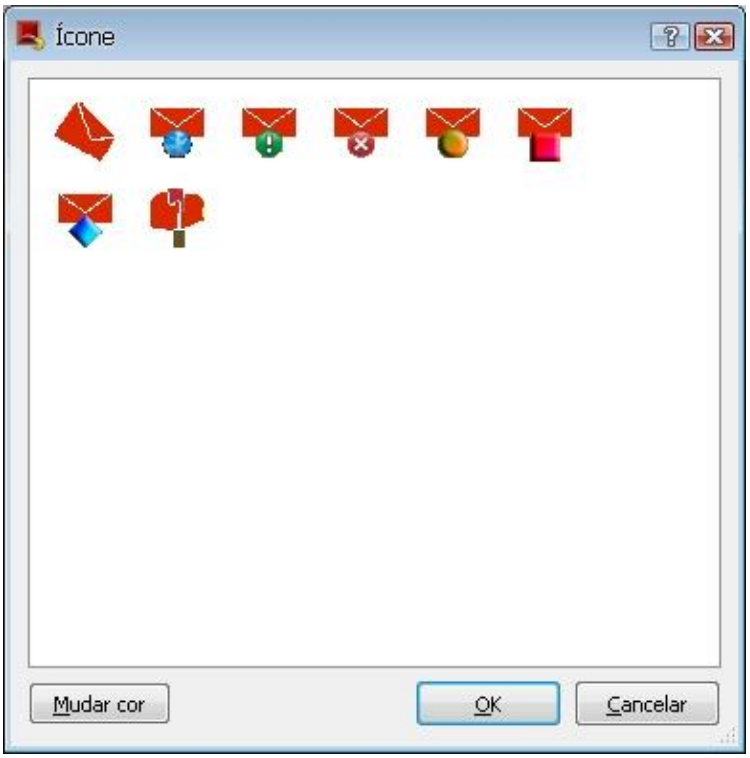

Figura 6. Editar Dispositivos Remotos – escolhas dos ícones.

Agora basta escolher o ícone que deseja utilizar. Se desejar mudar a cor é necessário selecionar o ícone desejado e clicar sobre o botão **"Mudar cor"** e escolher a nova cor dentro da paleta.

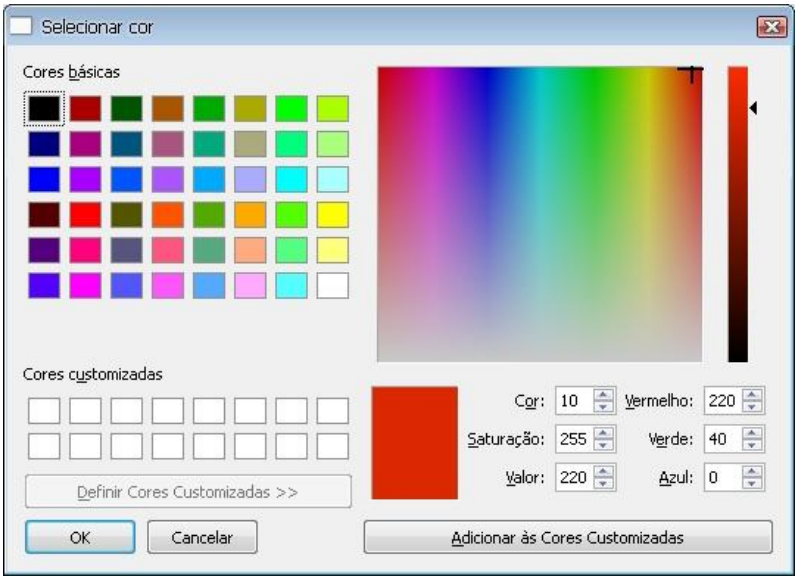

Figura 7. Editar Dispositivos Remotos – seleção da cor.

Clique em "**OK"** e feche as telas abertas até voltar à área de trabalho do Control Center. Este processo pode ser realizado quantas vezes forem necessárias e com todos os dispositivos gerenciados através do Control Center.

Chaves de Ativação

Esta opção permite atualizar a chave de ativação do ASMG e dos demais produtos que possam estar instalados juntos (apenas no caso do ASMG): Antivírus, Spam Meter e Web Content Analyzer.

Para visualizar ou atualizar a licença, deve-se:

- Clicar no botão *Licença* na barra de tarefas do ASMG que estiver conectado.

A janela de licença de ativação

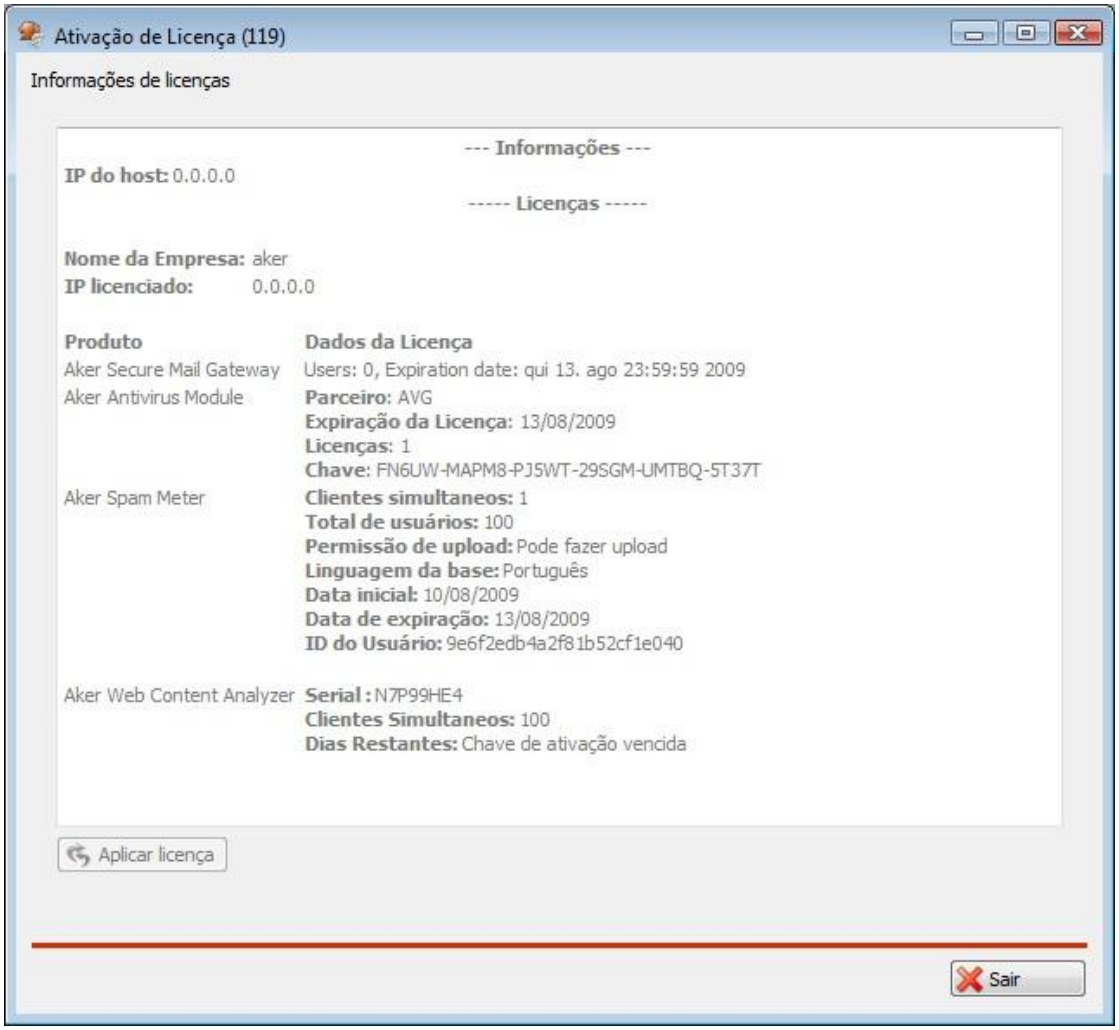

Figura 8. Informações sobre a licença de aplicação.

Esta janela é apenas informativa. Nela são mostrados todos os produtos que estão instalados junto com o ASMG e os dados referentes à licença de cada um deles. Entre estes dados pode-se verificar a data de expiração, número de licenças, etc, para cada produto.

Caso se deseje inserir uma nova licença, deve-se clicar no botão "**Carregar"**, localizado na barra de tarefas. Esta opção abrirá um diálogo onde se pode especificar o arquivo de onde a nova chave será carregada. No caso do ASMG, caso exista mais de um produto instalado junto com o ASMG, as chaves dos produtos adicionais também serão atualizadas.

Atualizações

O que são atualizações e onde consegui-lás?

Como todo software, o ASMG pode eventualmente apresentar bugs em seu funcionamento. À medida que estes problemas são resolvidos, a Aker produz um arquivo que permite a atualização de seu ASMG e a eliminação destes erros. Algumas vezes também são adicionadas determinadas características novas em uma versão já existente, de modo a aumentar sua performance ou aumentar sua flexibilidade.

Em ambos os casos, os arquivos de atualização ou correção são disponibilizados de forma gratuita no site da Aker: basta procurar o menu ***"Download"*** e selecionar a opção ***"Correções e Atualizações"***. Estes arquivos são sempre cumulativos, ou seja, é necessário apenas baixar a última versão disponível e esta incluirá as correções presentes nos arquivos de correção/atualização anteriores.

A janela de atualizações

Esta opção permite aplicar uma atualização ou correção do ASMG remotamente, através da interface gráfica. É possível também atualizar completamente a versão do produto. Para ter acesso à janela de atualizações deve-se clicar no ícone localizado na barra de ferramentas. Automaticamente a janela será aberta, para que sejam escolhidas as atualizações a serem aplicadas.
Essa janela se divide em duas abas: "**Atualização"** e **"Histórico"**, conforme explicadas a baixo:

© Aker Security Solutions

Aba Sistema de Atualização:

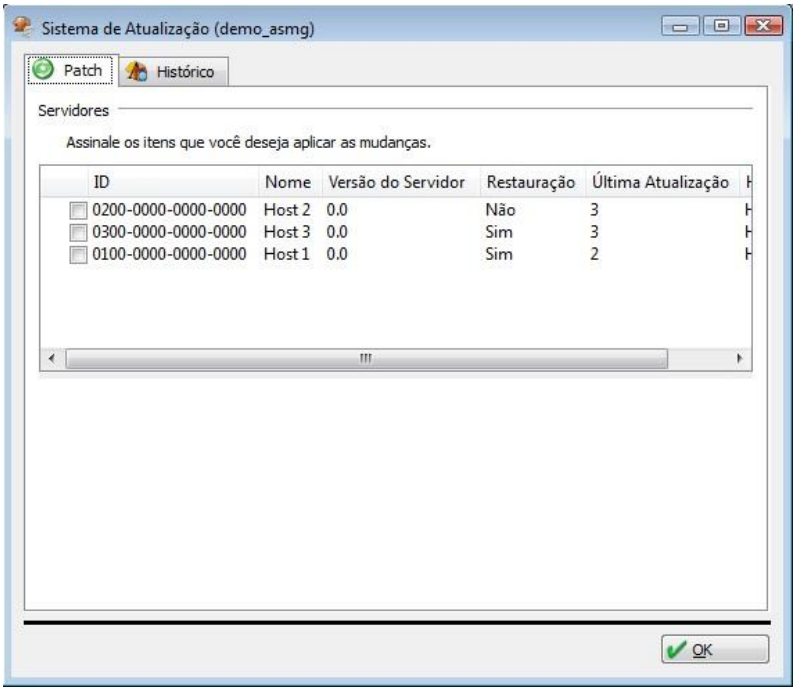

Figura 9. Sistema de atualizações ou correção do ASMG.

Por meio desta janela é possível visualizar o status atual das atualizações/correções aplicadas no ASMG. Caso se trate de cluster a janela apresentará as informações das máquinas que o compõem. Possui os seguintes campos:

- **Id**: Refere-se à identificação das máquinas que compõe o cluster;
- **Nome**: Refere-se ao apelido atribuído às máquinas;
- **Restauração**: Este campo informa se a última atualização aplicada pode ser desfeita.

As atualizações aplicadas por meio dos Patches e dos Hotfixes são alterações que podem ser desfeitas. Essa opção permite desfazer a última atualização aplicada na máquina, seja hotfix ou patch. Deve-se observar que as alterações são desfeitas uma por uma, ou seja, se a versão já estiver no Patch 3, e deseja-se voltar a versão inicial, deve ser desfeito o patch 3, depois o patch 2, e assim por diante.

Última atualização: Identificação do último patch aplicado no membro do cluster.

Hotfixes: Lista de hotfixes aplicados dentro do patch. Esta lista, mostra a ordem direta de aplicação dos hotfixes.

O hotfix é uma pequena atualização ou correção feita para um patch específico. Pode ser aplicado independente da ordem, o que não acontece com o patch, que deve ser aplicado na ordem seqüencial de atualização.

Caso a atualização ou correção sejam destinadas a uma versão diferente de sistema operacional ou de versão do ASMG, então o botão Aplicar ficará desabilitado, não permitindo sua aplicação.

Para carregar um arquivo de atualização ou correção deve-se clicar no ícone que se encontra na barra de ferramentas. Com isso é aberta uma janela, que permite carregar um arquivo de atualização do patch ou do hotfix, conforme mostra a figura abaixo.

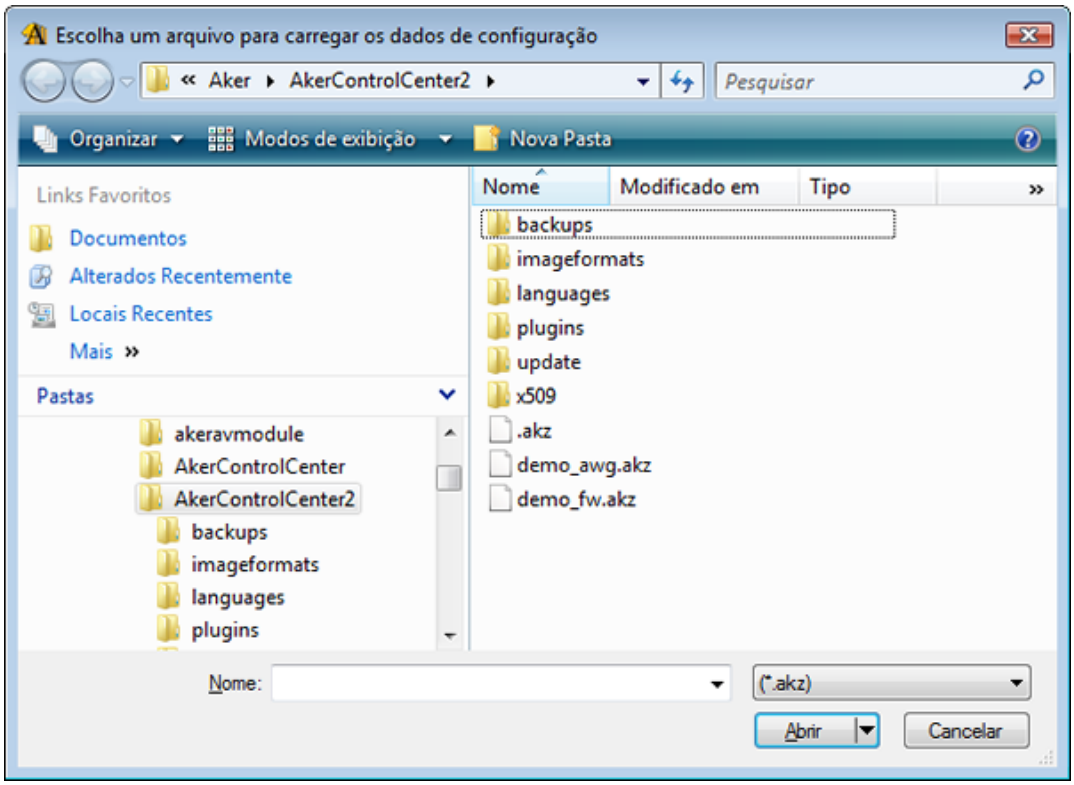

Figura 10. Escolha do arquivo para carregar os dados de configuração.

Para aplicar o arquivo de atualização/correção, deve-se primeiramente selecionar uma máquina na aba Patch, e logo em seguida clicar no ícone para que o patch ou o hotfix seja aplicado.

Caso queira aplicar o rollback, pelo menos uma máquina deve ser selecionada na aba Patch, e logo em seguida deve-se clicar no ícone , sendo que essas alterações serão desfeitas uma a uma, na sequência que foram atualizadas.

Para aplicar rollback em mais de uma máquina ao mesmo tempo, as mesmas devem estar com a mesma atualização, por exemplo: todas estão com a versão patch 3, e quer voltar para o patch 1.

- **Aba Histórico**

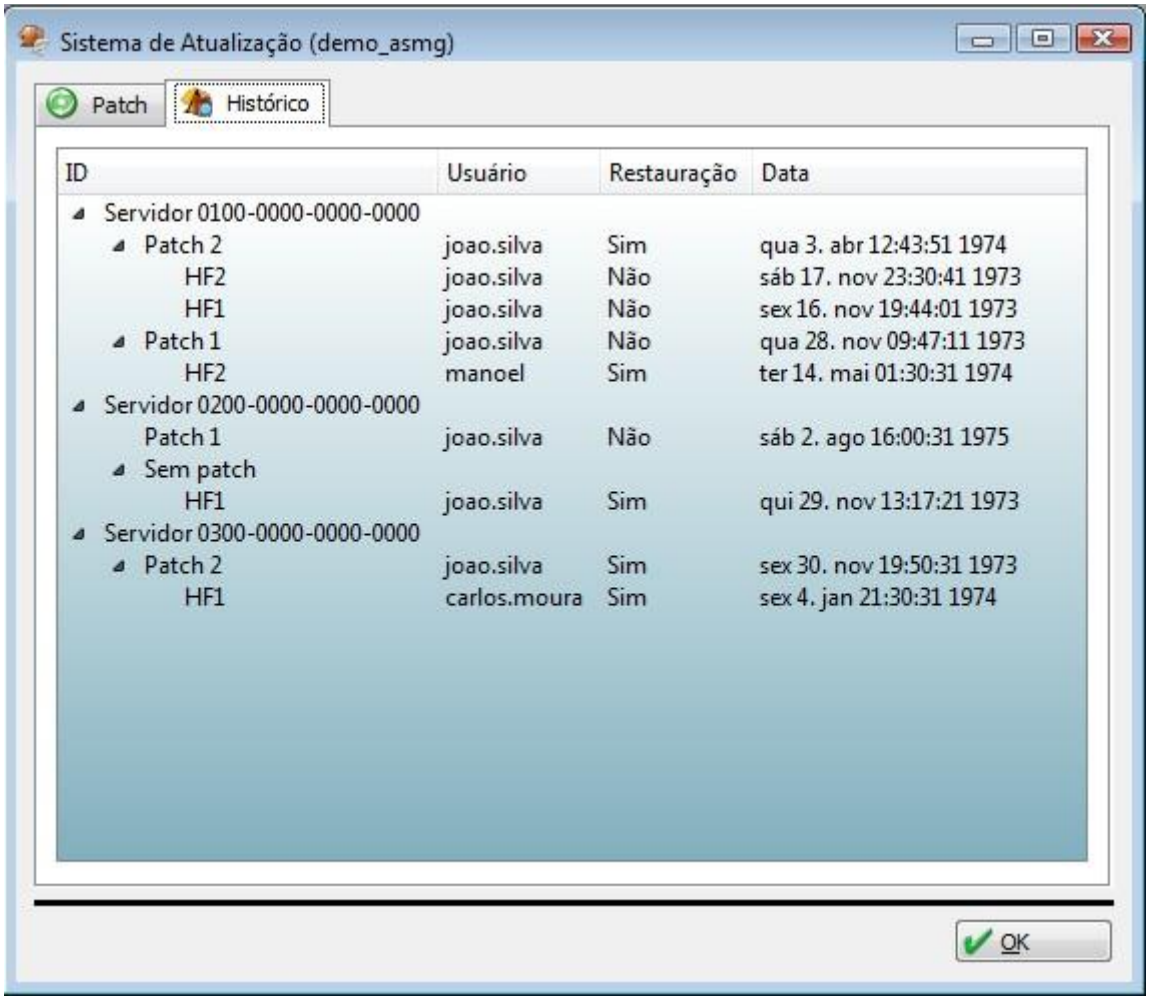
Sistema de Atualização (demo_asmg)
Patch
Histórico
ID
Usuário
Restauração
Data
Servidor 0100-0000-0000-0000
Patch 2 joao.silva Sim qua 3. abr 12:43:51 1974
HF2 joao.silva Não sáb 17. nov 23:30:41 1973
HF1 joao.silva Não sex 16. nov 19:44:01 1973
Patch 1 joao.silva Não qua 28. nov 09:47:11 1973
HF2 manoel Sim ter 14. mai 01:30:31 1974
Servidor 0200-0000-0000-0000
Patch 1 joao.silva Não sáb 2. ago 16:00:31 1975
Sem patch
HF1 joao.silva Sim qui 29. nov 13:17:21 1973
Servidor 0300-0000-0000-0000
Patch 2 joao.silva Sim sex 30. nov 19:50:31 1973
HF1 carlos.moura Sim sex 4. jan 21:30:31 1974
OK

Figura 11. Sistema de atualização – histórico.

Essa aba permite visualizar todo o histórico das aplicações dos patches e hotfixes.

A aba é composta dos seguintes campos:

ID: Mostra a identificação da máquina de onde foi feita a atualização.

Usuário: Indica o usuário que aplicou a atualização.

Restauração: Indica se pode ser ou não desfeito a atualização.

Data: Indica a data que foi feita alguma aplicação de patch ou hotfix.

A expressão "Versão Corrente" significa que não foi aplicado nenhum patch. Ao clicar no botão OK, o Patch ou o Hotfix não são aplicados, somente é fechada a janela.

O protocolo SMTP

3. O protocolo SMTP

*Entender o protocolo SMTP constitui uma base importante para compreender o funcionamento do **ASMG**. Para facilitar o entendimento da ferramenta, este capítulo fará uma pequena apresentação sobre o referido protocolo.*

Definição

O SMTP, ou Simple Mail Transfer Protocol é o protocolo padrão para envio de mensagens eletrônicas pela Internet. Foi proposto inicialmente pela IETF (*Internet Engineering Task Force*) em meados dos anos 80, mas com o passar do tempo, novas necessidades obrigaram que passasse por uma modernização, incluindo no protocolo funcionalidades extras ao modelo inicial. Atualmente é regulamentado pela RFC 2821 que, entre outras coisas propôs melhorias e novas extensões a serem suportadas, além das melhores práticas na implementação do serviço. Uma das premissas mais importantes é a interoperabilidade. Assim, mesmo que novas versões sejam lançadas, todos os servidores de correio que utilizem o SMTP como protocolo padrão devem suportar tanto as versões mais antigas quanto a mais atual.

Pela definição original do protocolo, a mensagem de correio é composta por um texto em formato ASCII e deve possuir cabeçalho e corpo, separados por uma linha em branco (vazia). No cabeçalho estão especificadas algumas informações de controle, ou seja, informações necessárias para indicação de origem, destino, assunto e trajeto, entre outras.

Para acomodar os vários tipos de arquivos contendo informações não-textuais, tais como imagens, sons e animações, que circulam anexados às mensagens de correio, a IETF (*Internet Engineering Task Force)* definiu o padrão MIME – *Multi-Purpose Internet Mail Extensions*, que é o formato utilizado para a identificação e codificação de vários conteúdos, a fim de padronizar as transmissões de mensagens, de forma que todos os MTAs consigam interpretá-las. Este padrão prevê a codificação de anexos que possuam como conteúdo caracteres não-ASCII ou binários, e a inclusão dessas versões codificadas no corpo da mensagem como se fossem anexos. Desta maneira, os servidores continuam a ver o corpo de cada mensagem como um texto ASCII, conforme a definição original.

Mensagem e Envelope

Uma boa analogia ao sistema de correio eletrônico é compará-lo ao sistema de correio convencional: quando desejamos enviar uma carta para alguém, colocamos a mensagem dentro de um envelope, onde informamos tanto os nossos dados (remetente), quanto os dados da pessoa que vai receber a carta (destinatário), ou seja, seu nome e dados completos para entrega. Se os dados do destinatário não forem preenchidos corretamente, não será possível fazer a entrega e a carta nos será devolvida, caso os dados constantes no envelope também estejam corretos.

© Aker Security Solutions

Já no sistema de correio eletrônico a diferença é que todo este processo de transferência da mensagem é feito de maneira eletrônica. Assim, precisamos ter uma conta de correio da Internet para que possamos enviar a mensagem e precisamos conhecer o endereço correto da pessoa para quem desejamos mandá-la, para que o encaminhamento necessário seja feito.

Quando enviamos uma mensagem, todo seu conteúdo é encapsulado por um envelope, onde é informado o endereço do remetente, a lista de destinatários e dados sobre extensões que são suportadas pelo protocolo. Os dados do envelope são utilizados pelos agentes de transporte de mensagem (MTA) para fazer o roteamento adequado das mensagens.

O envelope contém a mensagem que, por sua vez, é dividida em cabeçalho e corpo. O cabeçalho contém informações de controle, tais como a origem, remetente e destinatário, além de outros parâmetros necessários para a identificação e formatação da mensagem pelo programa de leitura usado pelo receptor. Já o corpo da mensagem contém a mensagem propriamente dita.

Alguns mecanismos de autenticação como o SPF e o Sender ID, e softwares anti-spam costumam analisar as informações existentes no envelope da mensagem para tentar identificar as possíveis mensagens indesejadas e, assim, filtrá-las. Mais detalhes sobre estes mecanismos serão vistos na Autenticação **SPF e Sender ID**.

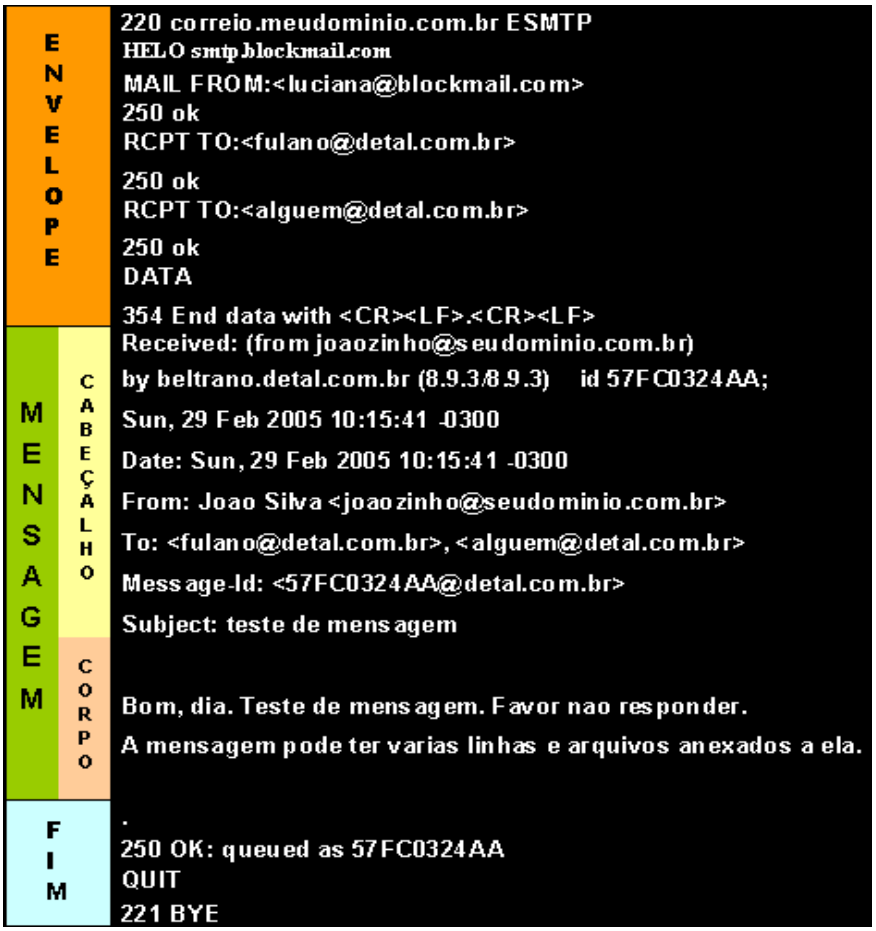

Figura 12. Mensagem e envelope.

Mail Exchange

Quando desejamos enviar um e-mail para alguém, temos que saber duas coisas importantes: seu nome de usuário (**1)** e o domínio para onde a mensagem deve ser encaminhada (**2)**. Os endereços eletrônicos obedecem a esta regra e possuem o seguinte formato:

1-username 2-nomedominio.com.br

username@nomedominio.com.br

Domínios são nomes que identificam um ou mais endereços IP, de maneira mnemônica. Apesar de nomes serem mais fáceis para o ser humano recordar, a Internet é toda baseada em endereços IP, e por isso é necessário um serviço que faça a conversão do nome do domínio para seu respectivo endereço IP. Este serviço é o DNS, ou *Domain Name Service*. Os registros DNS estão organizados em grandes bases de dados, hierarquicamente, de maneira que as conexões são roteadas de acordo com a entidade que gerencia aquela faixa de registros.

O MX (*Mail Exchange)* é um tipo de registro especial inserido no DNS de um domínio, que identifica o(s) servidor(es) responsável(is) por atender suas requisições de correio. Quando o emissor precisa encaminhar uma mensagem, faz uma pesquisa DNS para localizar o MX referente àquele domínio, e o resultado traz a relação dos servidores que estão habilitados a receber as mensagens direcionadas a ele. Como podem ser alocados mais de um servidor para resolver o MX de um determinado domínio, é possível ainda indicar a ordem de preferência entre eles para o recebimento de mensagens.

```
C:\>nslookup -querytype=mx meudominio.com.es

algumdominio.com.es  MX preference = 10   mail exchanger = mail1.XPTO.com
algumdominio.com.es  MX preference = 10   mail exchanger = mail2.XPTO.com
```

Figura 13. Exemplo de consulta pelo nslookup.

Pelo exemplo acima, podemos ver que para o domínio *meudominio.com.es* foram definidos dois servidores responsáveis por receber suas mensagens de correio, e que ambos possuem o número 10 para indicar a preferência. Neste caso, está estabelecido que ambos têm igual prioridade para responder pelo recebimento de mensagens direcionadas para *meudominio.com.es* .

Funcionamento

Pode-se resumir o funcionamento do SMTP da seguinte forma: quando um cliente SMTP tem uma mensagem a transmitir, estabelece um canal de transmissão em duas vias com o servidor SMTP de destino e encaminha a mensagem, que é repassada para a caixa de correio do usuário.

© Aker Security Solutions

Conforme a RFC 2821, a maior responsabilidade de um cliente SMTP é transferir as mensagens de correio para um ou mais servidores, ou então informar se ocorreu algum problema na tentativa de entrega. Para encontrar o servidor de destino correto, o cliente faz uma busca em vários registros DNS a fim de encontrar o MX responsável por aquele domínio. A partir daí, a transferência da mensagem pode ocorrer através de uma simples conexão com o servidor de destino, ou então por vários saltos (hops) através de outros servidores intermediários.

Quando o cliente necessita encaminhar uma mensagem, localiza o **MX** do servidor de destino e inicia um *handshake*, seguido por uma série de comandos que especificam o remetente, destinatário e o conteúdo da mensagem propriamente dito (incluindo cabeçalhos e outras estruturas). Durante a negociação de envio da mensagem, para cada comando enviado deve haver uma resposta indicando:

- Se o comando enviado foi aceito ou;
- Informações acerca de outros comandos adicionais que podem ser esperados, ou;
- Se existe algum erro permanente ou temporário que impeça a transmissão da mensagem.

Quando a transmissão é finalizada, podem ocorrer duas situações: a conexão é encerrada, ou então o cliente pode iniciar outras transações.

Um remetente pode enviar simultaneamente varias cópias de uma mensagem para diferentes destinatários, utilizando o conceito de lista de distribuição (um nome que identifica um grupo de usuários). Caso isto aconteça com vários usuários do mesmo destino, apenas uma cópia será encaminhada para o servidor, que se encarrega de enviar uma cópia para todos os destinatários.

Erros de Transmissão

Durante a transmissão de uma mensagem, podem acontecer situações em que ela não consegue ser entregue. Os motivos para esta condição são variados e podem ocorrer por conta de problemas temporários ou permanentes. De acordo com a RFC 2821, servidores que implementam o protocolo SMTP devem estar preparados para lidar com estas situações e, normalmente, o remetente da mensagem recebe uma notificação de falha, contendo o código de erro e sua respectiva explicação.

3..1. Erros Temporários

Geralmente, quando o emissor recebe uma mensagem de erro temporário vinda do receptor, tenta enviar a mensagem novamente dentro de algum tempo, até o prazo máximo de cinco dias. Esses erros de transmissão podem acontecer por vários motivos. Dentre eles podemos citar problemas na comunicação entre emissor e receptor, falta de espaço em disco do receptor para armazenar a mensagem, ou até mesmo devido a simulações de erro por parte do servidor para validar se a

mensagem vem de fonte confiável ou não. O **ASMG** implementa esta última política, conhecida como *Graylist*.

Os códigos de erro temporários mais importantes são os seguintes:

- **421 – Service not available, closing transmission channel.** (Serviço indisponível, fechando o canal de transmissão);
- **451 – Requested action aborted: local error in processing.** (Ação solicitada cancelada: erro local no processamento);
- **452 – Requested action not taken: insufficient system storage.** (Ação requisitada não concluída: espaço de armazenamento insuficiente).

3..2. Erros Permanentes

Quando este tipo de erro ocorre, significa dizer que a mensagem foi rejeitada pelo receptor e não haverá nova tentativa por parte do emissor de tentar entregá-la. Dentre os tipos de erro mais comuns, podemos citar o endereço de envio incorreto, caixa do destinatário sem espaço disponível, além de outros motivos ligados à prática de spam, como inserção do servidor em blacklists, verificação SPF inválida, etc.

Os códigos de erro permanente mais importante são os seguintes:

- **550 – User Unknown.** (Usuário desconhecido).
- **552 – Requested mail action aborted: exceeded storage allocation.** (Ação de envio solicitada abortada: espaço de armazenamento excedido).
- **557 – Access denied** . (Acesso negado à Erro permanente para endereço reverso não encontrado ou inválido).

Comandos SMTP

A seguir, vamos listar alguns dos comandos mais importantes do protocolo SMTP referentes à implementação de um MTA, citando seu significado e utilização:

- **HELO (HELLO) – obrigatório:** identifica o Emissor da mensagem para o Receptor;
- **MAIL FROM – obrigatório:** identifica o remetente da mensagem, que será utilizado pelos servidores de trânsito;
- **RCPT TO (ReCiPienT) – obrigatório:** este comando identifica o destinatário da mensagem. Caso haja mais de um destinatário, o comando deve ser repetido quantas vezes forem necessárias;
- **DATA – obrigatório:** inicia a transmissão da mensagem. O conteúdo da mensagem é transmitido logo em seguida, usando qualquer um dos 128 caracteres ASCII. O fim da transmissão é especificado por uma seqüência **"<CRLF>.<CRLF>"**;

© Aker Security Solutions

- **RSET (ReSET) – obrigatório:** determina que a transmissão atual deverá ser abortada. Todos os dados referentes são descartados.
- **VRFY (VeRiFY):** solicita ao Receptor a confirmação de que o argumento identifica um usuário conhecido. Se for identificado o nome completo do usuário é retornado (se este possuir) e a transmissão concluída;
- **EXPN (EXPaNd):** solicita ao Receptor a confirmação de que o argumento identifica uma lista de e-mails. Se for identificada serão retornados os membros desta lista no mesmo formato retornado pelo comando VRFY;
- **NOOP – obrigatório:** não possui efeitos ou parâmetros. Apenas faz com que o receptor envie um OK;
- **QUIT – obrigatório:** determina que o Servidor envie um OK e então feche o canal de comunicação com o Cliente.

O início da comunicação entre dois computadores acontece com um *handshake* de três vias:

O Cliente (client) envia um pacote de dados ao Servidor (server), requisitando a abertura de uma conexão. Assim que recebe a resposta, o Servidor pode enviar uma resposta favorável ou não ao cliente. Se a resposta à conexão for desfavorável (REJECT), a conexão é encerrada. Caso seja favorável (ACCEPT ACK), o cliente inicia a transmissão.

© Aker Security Solutions

Conceitos importantes

4. Conceitos importantes

*Por padrão, o **ASMG** utiliza uma política restritiva de bloqueio de mensagens no repasse, afinal, conforme já mencionado, a ferramenta atua como intermediário em seu recebimento. Isso significa dizer que toda mensagem vinda de um agente remoto será recusada se não houver a liberação explícita do mesmo para que este faça o repasse da mensagem utilizando o **ASMG**.*

*Para melhor entendimento de algumas funções, neste capítulo vamos conceituar alguns termos importantes para o melhor entendimento do **ASMG**.*

Clientes conhecidos e desconhecidos

Consideremos que um cliente é um programa que tenta enviar uma mensagem de e-mail que é interceptada pelo **ASMG**. Para que este cliente seja considerado "conhecido" e, tenha a sua conexão aceita sem restrição, é necessário que obedeça a qualquer uma das condições a seguir:

- Pertença a um domínio (por DNS reverso) cadastrado na configuração de repasse por domínios, ou
- Pertença a uma rede cadastrada na configuração de repasse por redes, ou
- Possua um endereço IP cadastrado na configuração de repasse por servidores ou
- Tenha realizado autenticação SMTP (a qual será visto a seguir).

Caso não obedeça a nenhuma destas condições, o cliente é chamado "desconhecido". Os clientes conhecidos podem enviar mensagens para qualquer domínio. Já os desconhecidos podem enviar mensagens apenas para domínios conhecidos pela ferramenta. O **ASMG** reconhece domínios em duas situações:

- O domínio está cadastrado na configuração de repasse por domínios, ou
- O servidor onde se encontra o produto está configurado como MX autorizado do domínio em questão, no DNS acessado por ele.

Autenticação SPF e Sender-ID

É fato que os spammers estão usando técnicas cada vez mais sofisticadas, buscando "furos" no protocolo SMTP que acolham suas técnicas invasivas. Já é de conhecimento geral que o protocolo SMTP não possui mecanismo de autenticação própria, deixando que as camadas superiores façam o controle necessário. Assim, os spammers exploram esta vulnerabilidade para, dentre outras práticas, enviar e-

mails em nome de outras pessoas ou como se pertencessem a determinado domínio.

Um caso muito comum hoje em dia é o *spoofing*: um usuário **X** recebe uma mensagem vinda de um remetente **Y** quando, na verdade, **Y** não enviou nenhuma mensagem. Ou seja, alguém se fez passar por **Y** e enviou mensagens em seu nome. Casos de mensagens enviadas através de endereços forjados ou inexistentes são um grande problema quando há a necessidade de rastreá-las e descobrir suas origens. Esta vulnerabilidade torna necessário um mecanismo de autenticação externa a fim de assegur se a fonte da mensagem é real ou não.

Outra prática muito comum tem sido o *phishing*: um spammer se faz passar por uma determinada empresa ou entidade comercial e induz o usuário a fornecer informações de caráter privado, tais como senhas de banco, números de cartão de crédito ou CPF, que serão utilizados para transferências bancárias ilícitas, e-commerce ou outros tipos de fraudes. Normalmente estas mensagens trazem links falsos ou solicitam que o destinatário cadastre-se em determinada página. Alguns casos recentes de *phishing* foram tão perfeitos que estes links maliciosos eram cópias exatas dos sites das empresas verdadeiras, incluindo padrões de cores e fontes.

Os dois padrões atualmente propostos para tentar neutralizar esta falha de segurança e combater estes ataques são o **SPF** (*Sender Policy Framework*) e o *Sender-ID.* Nesta seção será explicado os dois padrões, trazendo seus conceitos, notícias atuais quanto à utilização, seus prós e contras.

4..1. Padrão SPF

Criado em junho de 2003, o padrão **SPF** foi uma alternativa proposta por um grupo de pesquisa anti-spam, o *The Anti-Spam Research Group* (ASRG), ao *MTA Authorization Records in DNS* (MARID), grupo ligado à IETF, responsável por tentar restringir os problemas causados pela falta de autenticação do protocolo SMTP.

Este padrão permite que, através de uma configuração simples no MX de determinado domínio (*meudominio.com.br* , por exemplo), seja adicionada uma linha de texto com a informação que descreve quais os endereços dos servidores de e-mail que estão autorizados a enviar mensagens referentes àquele domínio (MX-reverso). Quando um spammer forja um endereço de e-mail para enviar mensagens, precisa conectar-se a um servidor que permita este repasse indevido para só então poder enviá-la. Se o servidor de destino estiver utilizando o padrão de autenticação SPF, assim que receber a mensagem pode perguntar ao servidor que responde pelo domínio do endereço forjado se a mensagem realmente partiu de lá. Desta maneira, é possível certificar-se se quem mandou é quem realmente diz ser e, caso não seja, descartar a mensagem.

Exemplificando: um spammer envia uma mensagem para um grupo de endereços assumindo a identidade de *mariazinha@meudominio.com.br*. Os MTAs que possuem o SPF configurado em seus servidores de correio fazem uma verificação simples para identificar se tanto o IP como o domínio do remetente que enviou

aquela mensagem realmente correspondem ao IP relacionado no MX que responde por aquele domínio para, desta maneira, validar se a mensagem partiu do endereço *mariazinha@meudominio.com.br*. Em caso positivo, a mensagem será entregue. Caso contrário será descartada.

Um exemplo típico de registro a ser colocado no DNS contém as seguintes informações:

- **"v="** define a versão do SPF que está sendo utilizada;
- **"mx":** endereço(s) do(s) servidor(es) válido(s) por responder pelo MX daquele domínio;
- **"ptr":** especifica que servidores cujo nome termine com *meudominio.com.br* possam enviar mensagens por aquele domínio. Este registro não é obrigatório;
- **"-all":** indica que se as verificações de MX e PTR não forem verdadeiras, a mensagem deve ser rejeitada como mensagem falsa.

Aplicando esta regra, teríamos a seguinte linha de comando:

meudominio.com.br IN TXT "v=spf1 mx ptr -all"

Esta prática é interessante principalmente porque torna possível descartar várias mensagens de origem duvidosa sem alocar grandes recursos de processamento. Além disso, podemos resguardar a rede interna quanto a possíveis ameaças de vírus, já que é comum usar remetentes falsos para encaminhar este tipo de mensagens. Devido à grande quantidade de SPAMs que circulam pela Internet, diversas entidades como a AOL, SAP, Terra Networks, GMail, Google, entre outros, já adotaram o padrão SPF para filtrar as mensagens. Além disso, softwares como o SpamAssassin, Postfix, Sendmail e Qmail já suportam ou disponibilizaram patches e plugins para o SPF.

Também temos que levar em conta que o SPF ainda não é um padrão adotado, apenas proposto. Pode levar certo tempo até ser adotado em massa e até lá, vários servidores ainda terão que adequar-se. Enquanto isso, se o DNS de determinado servidor de envio não tiver o SPF configurado nenhuma ação será tomada e a mensagem será entregue normalmente. Apesar de ser uma abertura no sistema, ainda é necessário aguardar certo consenso para realizar todas as modificações necessárias.

4..2. Sender-ID

O Sender-ID também é um autenticador de mensagens de correio. Este padrão proposto pela Microsoft alia as características do padrão aberto SPF com uma tecnologia já anteriormente desenvolvida pela Microsoft, chamada Caller-ID ("Identificador de Chamadas"). O Sender-ID trabalha não apenas verificando o endereço de quem enviou a mensagem, mas também detectando seu remetente e facilitando a filtragem do lixo eletrônico.

Funciona da seguinte maneira: cada domínio possui um nome associado a um endereço IP e ambos estão inclusos em um banco de dados, denominado Domain Name System (DNS). Pelo DNS, podemos obter o endereço IP de destino, apenas fornecendo o nome de domínio (o inverso é chamado DNS reverso). Após receber uma mensagem, o servidor de destino faz uma pesquisa DNS para validar se o servidor de onde a mensagem foi originada está cadastrado como MX responsável por aquele domínio. Em seguida, o Sender-ID valida o remetente da mensagem. Caso alguma das verificações falhe, a mensagem será descartada. Caso contrário será entregue.

O projeto que deu início ao Sender-ID começou com a ajuda de diversos parceiros de renome, entre eles várias distribuições do Linux, ISPs e desenvolvedores de softwares para correio eletrônico. No ano passado foi submetido à IETF, mas há várias discordâncias quanto à sua aceitação, tendo em vista que a Microsoft quer cobrar os direitos sobre o licenciamento da tecnologia, o que impede que seja adotada pela comunidade do software livre.

© Aker Security Solutions

Instalação

5. Instalação

Requisitos de hardware e software

Para o ASMG

O Aker Secure Mail Gateway roda sobre o sistema operacional proprietário, em plataformas Intel ou compatíveis.

Para que o Aker Secure Mail Gateway execute de maneira satisfatória todos os componentes de hardware é necessário possuir as seguintes configurações:

- Computador Intel ou compatível 1.0 GHz ou superior;

  Para utilizar um link com alta taxa de transferência ou utilizar criptografia em um link com velocidade relativamente alta, recomenda-se o uso de um computador mais potente.

- 512 Mbytes de memória RAM;

  Para fazer um grande uso dos serviços de proxy e de criptografia, provavelmente será necessário utilizar memória maior ou igual a 512 Mbytes.

- 20 Gbytes de espaço em disco;

  Para armazenar os logs do sistema por um grande espaço de tempo recomenda-se o uso de um disco maior.

- Leitor de CD-ROM, monitor, mouse e teclado;

  Isso só é necessário durante a instalação ou caso se pretenda utilizar a interface texto a partir do console, entretanto é altamente recomendado em todos os casos.

- Placa(s) de rede.

  Não existe um número máximo de placas de rede que podem ser colocadas no Firewall. A única limitação existente é a limitação do próprio hardware. Caso necessite de um grande número de interfaces de rede, pode-se optar por placas com mais de uma saída na mesma interface.

Para a interface gráfica

A interface gráfica de administração do Aker Secure Mail Gateway roda em plataformas Windows, Linux em plataformas Intel ou compatíveis.

© Aker Security Solutions

Para que a interface gráfica execute de maneira satisfatória os componentes de hardware devem-se possuir as seguintes configurações:

- Computador Intel ou compatível 1.3Mhz ou superior;
- 256 Mbytes de memória RAM;
- 2 Gbytes de espaço livre em disco;
- Monitor;
- Mouse;
- Teclado;
- Placa de rede.

Todos os componentes do hardware devem ser suportados pelo sistema operacional na qual a interface será instalada, em alguma das versões aceitas pelo produto.

Instalando o Aker Secure Mail Gateway

O Aker Secure Mail Gateway pode ser adquirido na forma de appliance, i.e. Firewall Box. Sendo comprado desta forma, o produto já vem instalado e pré-configurado. Caso tenha optado por comprar apenas o software (versão IS), a instalação deverá ser feita na máquina escolhida, o que será explicado neste tópico.

Para instalá-lo deve-se iniciar a máquina com o CD-ROM de instalação ou com o PEN-DRIVER que podem ser efetuado o download no site da Aker.

Para gravar o PEN-DRIVER, siga os passos abaixo:

1. Efetuar o download do arquivo no site da Aker;
2. Verificar se o pen drive no Linux está com sdb, digitar o comando como root. “#dmesg | grep sd” ou “#fdisk –l” serão mostradas as informações de disco da máquina e encontre o pen-drive.
3. Após identificar em qual device o Linux montou o pen-drive, digitar o comando
   “dd if=<nome do arquivo que fez o download> | gunzip | dd of=/dev/<device que se encontra o pen-driver>”.
   Exemplo:

   “dd if=<aker-box-2.0-pt-installer.img.gz | gunzip | dd of=/dev/sdb”

4. Pronto. Seu pen-driver é um instalado dos produtos da Aker.

Após reiniciar a máquina o programa fwinst é o responsável por efetuar a instalação e a configuração do sistema para a execução do Aker Secure Mail Gateway. Ao ser executado, ele mostrará a seguinte tela:

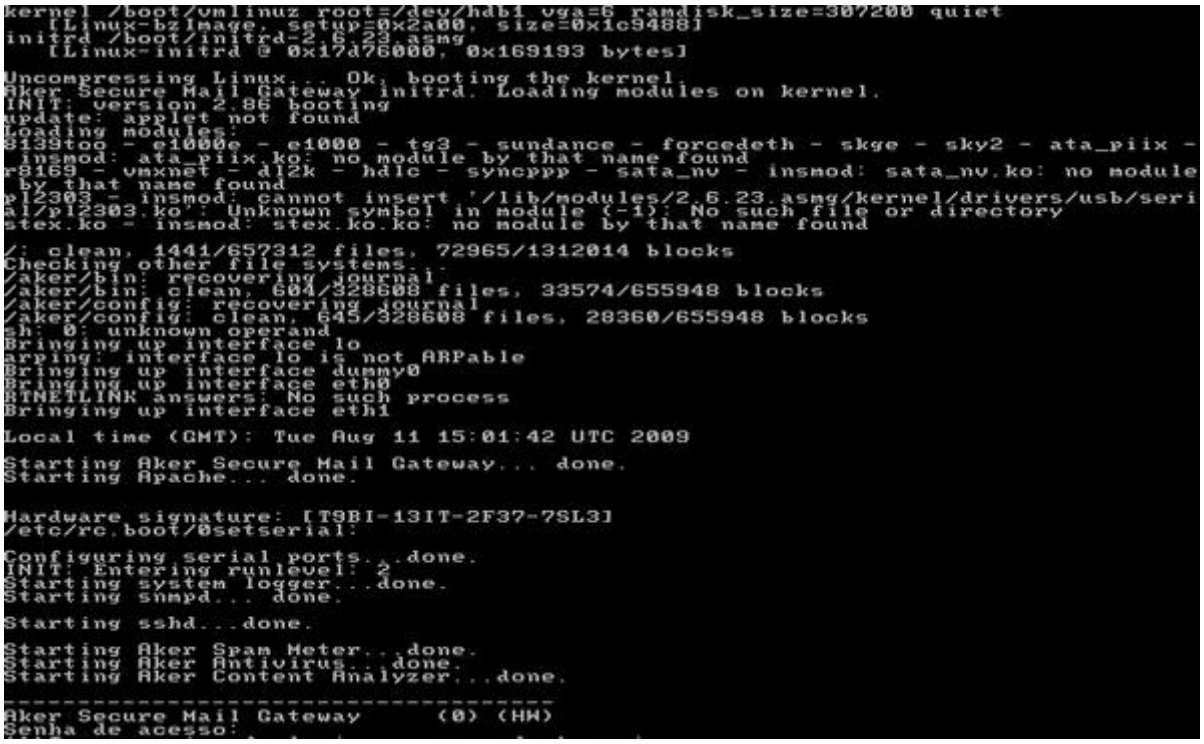
kernel /boot/vmlinuz root=/dev/hdb1 vga=6 ramdisk_size=307200 quiet
[Linux-bzImage, setup=0x2a00, size=0x1c9488]
initrd /boot/initrd-2.6.23.asmg
[Linux-initrd @ 0x17d76000, 0x169193 bytes]
Uncompressing Linux... Ok, booting the kernel.
Aker Secure Mail Gateway initrd. Loading modules on kernel.
INIT: version 2.86 booting
update: applet not found
Loading modules:
8139too - e1000e - e1000 - tg3 - sundance - forcedeth - skge - sky2 - ata_piix -
insmod: ata_piix.ko: no module by that name found
r8169 - vmxnet - d12k - hdlc - syncppp - sata_nv - insmod: sata_nv.ko: no module
by that name found
pl2303 - insmod: cannot insert '/lib/modules/2.6.23.asmg/kernel/drivers/usb/seri
al/pl2303.ko': Unknown symbol in module (-1): No such file or directory
stex.ko - insmod: stex.ko.ko: no module by that name found
/: clean, 1441/657312 files, 72965/1312014 blocks
Checking other file systems...
/aker/bin: recovering journal
/aker/bin: clean, 604/328608 files, 33574/655948 blocks
/aker/config: recovering journal
/aker/config: clean, 645/328608 files, 28360/655948 blocks
sh: 0: unknown operand
Bringing up interface lo
arping: interface lo is not ARPable
Bringing up interface dummy0
Bringing up interface eth0
RTNETLINK answers: No such process
Bringing up interface eth1
Local time (GMT): Tue Aug 11 15:01:42 UTC 2009
Starting Aker Secure Mail Gateway... done.
Starting Apache... done.
Hardware signature: [T9BI-13IT-2F37-7SL3]
/etc/rc.boot/0setserial:
Configuring serial ports...done.
INIT: Entering runlevel: 2
Starting system logger...done.
Starting snmpd... done.
Starting sshd...done.
Starting Aker Spam Meter...done.
Starting Aker Antivirus...done.
Starting Aker Content Analyzer...done.
Aker Secure Mail Gateway (0) (HW)
Senha de acesso:

Figura 14. Instalação do ASMG - fwinst.

Utilize a senha padrão "123456" para iniciar a instalação.

Aker Secure Mail Gateway
Este programa realiza a configuracao inicial do Aker Secure Mail Gateway v2.2
Nas proximas telas, algumas perguntas simples serao feitas, de forma
que seja possivel administrar o Gateway atraves de sua interface
grafica remota.
Pressione Enter para continuar._

Figura 15. Instalação do ASMG – mensagem de configuração inicial.

Neste ponto temos o contrato EULA para utilização dos produtos Aker, digite "S" para aceitar e continuar a instalação.

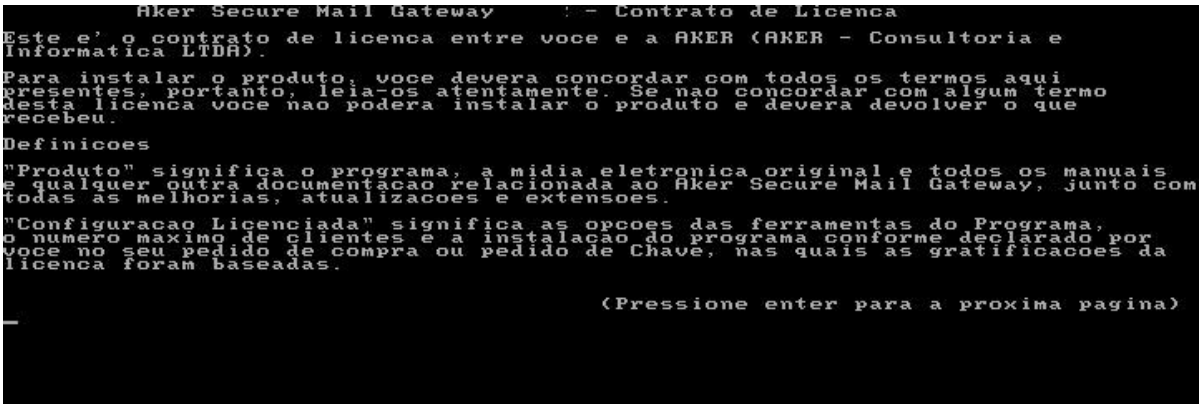
Aker Secure Mail Gateway : - Contrato de Licenca
Este e' o contrato de licenca entre voce e a AKER (AKER - Consultoria e
Informatica LTDA).
Para instalar o produto, voce devera concordar com todos os termos aqui
presentes, portanto, leia-os atentamente. Se nao concordar com algum termo
desta licenca voce nao podera instalar o produto e devera devolver o que
recebeu.
Definicoes
"Produto" significa o programa, a midia eletronica original e todos os manuais
e qualquer outra documentacao relacionada ao Aker Secure Mail Gateway, junto com
todas as melhorias, atualizacoes e extensoes.
"Configuracao Licenciada" significa as opcoes das ferramentas do Programa,
o numero maximo de clientes e a instalacao do programa conforme declarado por
voce no seu pedido de compra ou pedido de Chave, nas quais as gratificacoes da
licenca foram baseadas.
(Pressione enter para a proxima pagina)
_

Figura 16. Contrato de licença.

O próximo passo é efetuar as configurações de rede:

Aker Secure Mail Gateway
Para poder administrar o sistema remotamente e ativar a licenca,
e' necessario configurar ao menos uma placa de rede.

Figura 17. Configuração de rede.

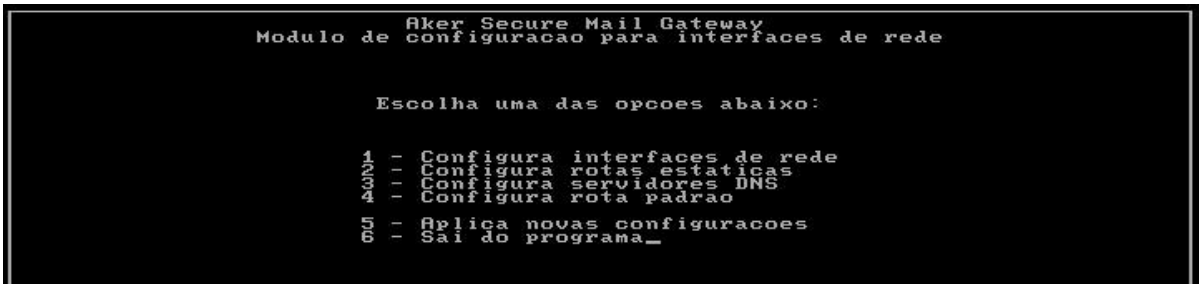
Aker Secure Mail Gateway
Modulo de configuracao para interfaces de rede
Escolha uma das opcoes abaixo:
1 - Configura interfaces de rede
2 - Configura rotas estaticas
3 - Configura servidores DNS
4 - Configura rota padrao
5 - Aplica novas configuracoes
6 - Sai do programa_

Figura 18. Módulo de configuração para instalação de rede.

Neste ponto criamos o usuário que permitirá a administração remota do Aker Secure Mail Gateway através da interface gráfica remota.

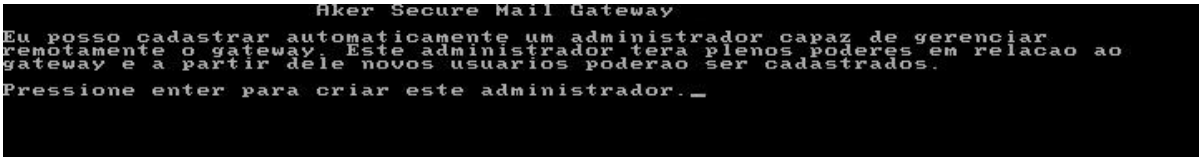
Aker Secure Mail Gateway
Eu posso cadastrar automaticamente um administrador capaz de gerenciar
remotamente o gateway. Este administrador tera plenos poderes em relacao ao
gateway e a partir dele novos usuarios poderao ser cadastrados.
Pressione enter para criar este administrador._

Figura 19. Mensagem de criação de administrador.

Pode-se criar um certificado para o servidor web contido no Aker Secure Mail Gateway, basta preencher os campos solicitados pelo instalador:

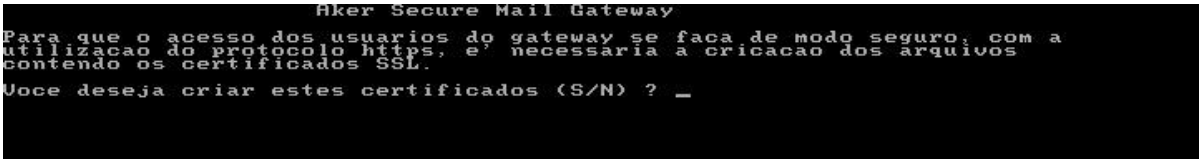
Aker Secure Mail Gateway
Para que o acesso dos usuarios do gateway se faca de modo seguro, com a
utilizacao do protocolo https, e' necessaria a cricacao dos arquivos
contendo os certificados SSL.
Voce deseja criar estes certificados (S/N) ? _

Figura 20. Mensagem de aceitação – criação de certificados.

Finalizando a instalação:

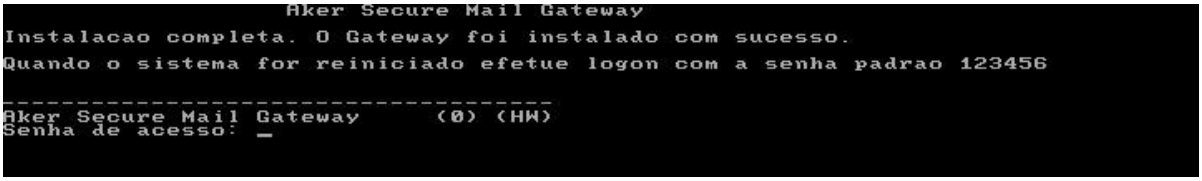
Aker Secure Mail Gateway
Instalacao completa. O Gateway foi instalado com sucesso.
Quando o sistema for reiniciado efetue logon com a senha padrao 123456
Aker Secure Mail Gateway (0) (HW)
Senha de acesso: _

Figura 21. Mensagem de instalação completa.

Instalação finalizada, agora basta iniciar as configurações através da interface gráfica.

Instalação da Interface Gráfica para Windows

A instalação da interface gráfica para Windows do ASMG compreende os seguintes passos:

Execute o arquivo de instalação AkerControlCenter-2.0.9-xx-win-AkerSecureMailGateway_2.5.0.exe.

A seguinte tela aparecerá. Pressione o botão "Avançar" para iniciar a instalação.

InstallShield Wizard do Aker Control Center - Mail GW
Aker Secure Mail Gateway
Bem-vindo ao InstallShield Wizard do Aker Control Center - Mail GW
O InstallShield Wizard irá instalar o Aker Control Center - Mail GW em seu computador. Para continuar, clique em Avançar.
AVISO: Este progama está protegido por lei de copyright e tratados internacionais.
Aker
Security Solutions
< Voltar
Avançar >
Cancelar

Figura 22. Instalação da Interface Gráfica para Windows.

Neste ponto, você deverá aceitar os termos do contrato da licença e pressionar "Avançar".

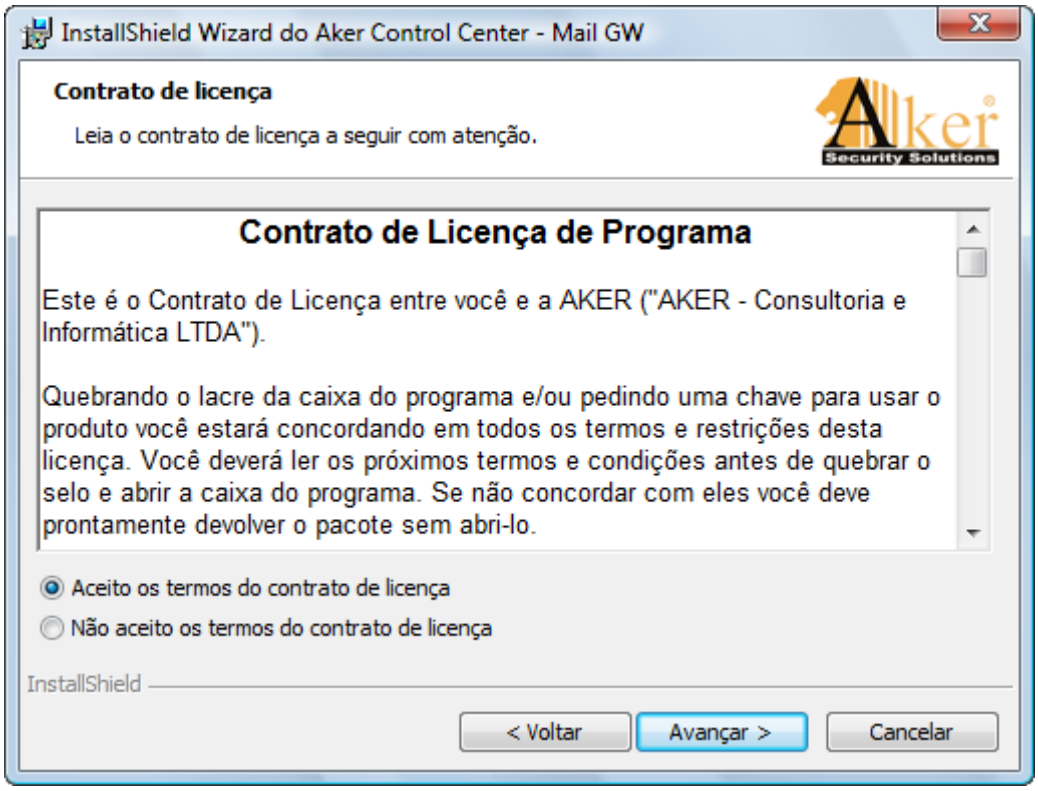
InstallShield Wizard do Aker Control Center - Mail GW
Contrato de licença
Leia o contrato de licença a seguir com atenção.
Contrato de Licença de Programa
Este é o Contrato de Licença entre você e a AKER ("AKER - Consultoria e Informática LTDA").
Quebrando o lacre da caixa do programa e/ou pedindo uma chave para usar o produto você estará concordando em todos os termos e restrições desta licença. Você deverá ler os próximos termos e condições antes de quebrar o selo e abrir a caixa do programa. Se não concordar com eles você deve prontamente devolver o pacote sem abri-lo.
Aceito os termos do contrato de licença
Não aceito os termos do contrato de licença
InstallShield
< Voltar
Avançar >
Cancelar

Figura 23. Instalação da Interface Gráfica para Windows - contrato.

Após isso, selecione a opção "Padrão" na tela abaixo e pressioner "Instalar" na tela seguinte.

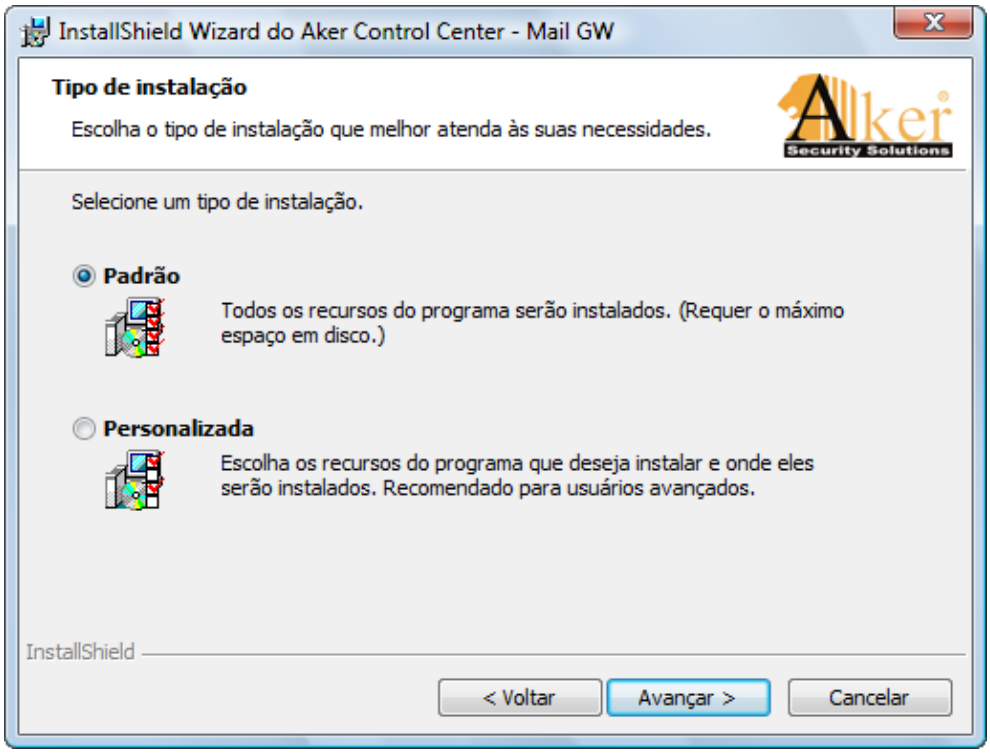
InstallShield Wizard do Aker Control Center - Mail GW
Tipo de instalação
Escolha o tipo de instalação que melhor atenda às suas necessidades.
Selecione um tipo de instalação.
Padrão
Todos os recursos do programa serão instalados. (Requer o máximo espaço em disco.)
Personalizada
Escolha os recursos do programa que deseja instalar e onde eles serão instalados. Recomendado para usuários avançados.
InstallShield
< Voltar
Avançar >
Cancelar

Figura 24. Tipo de instalação - padrão.

© Aker Security Solutions

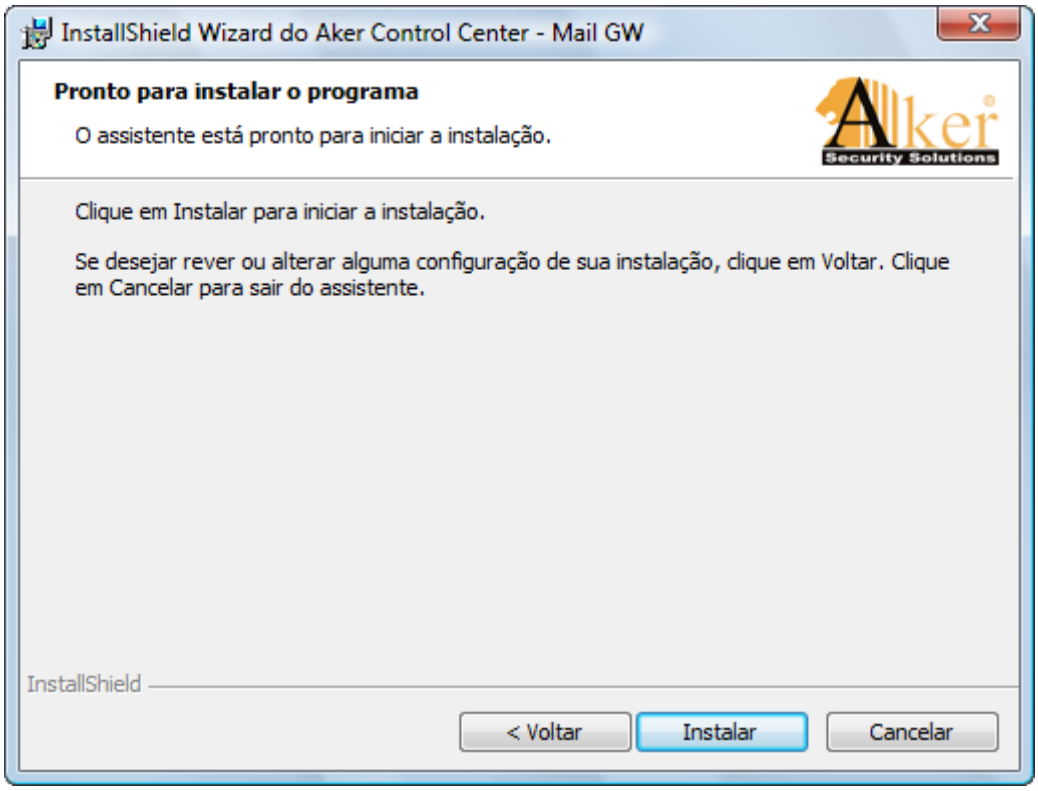
InstallShield Wizard do Aker Control Center - Mail GW
Pronto para instalar o programa
O assistente está pronto para iniciar a instalação.
Clique em Instalar para iniciar a instalação.
Se desejar rever ou alterar alguma configuração de sua instalação, clique em Voltar. Clique em Cancelar para sair do assistente.
InstallShield
< Voltar
Instalar
Cancelar

Figura 25. Mensagem de inicio de instalação.

Pronto. A instalação iniciará conforme a tela abaixo.

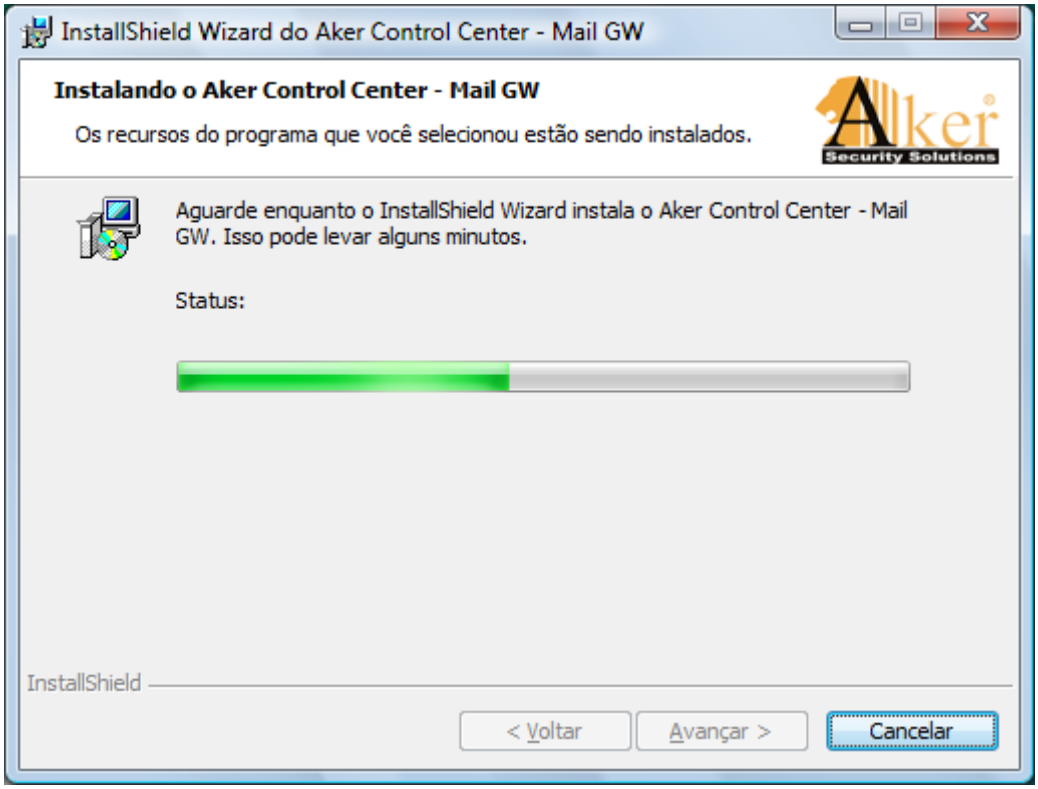
InstallShield Wizard do Aker Control Center - Mail GW
Instalando o Aker Control Center - Mail GW
Os recursos do programa que você selecionou estão sendo instalados.
Aguarde enquanto o InstallShield Wizard instala o Aker Control Center - Mail GW. Isso pode levar alguns minutos.
Status:
InstallShield
< Voltar
Avançar >
Cancelar

Figura 26. Status de instalação do Aker Control Center.

© Aker Security Solutions

Neste ponto, a tela abaixo surgirá. Pressione "Concluir" para finalizar a instalação.

InstallShield Wizard do Aker Control Center - Mail GW
Aker Secure Mail Gateway
Conclusão do InstallShield Wizard do Aker Control Center - Mail GW
O InstallShield Wizard instalou com sucesso o Aker Control Center - Mail GW. Clique em Concluir para sair do InstallShield Wizard.
Aker
Security Solutions
< Voltar
Concluir
Cancelar

Figura 27. Mensagem de conclusão de instalação.

Configuração

6. Configuração

A fim de facilitar a administração da ferramenta, esta foi dividida em várias partes, cada uma englobando uma funcionalidade específica. Os conhecimentos adquiridos no Tópico "**Sobre o Aker Control Center"**, e o papel desempenhado pelas Entidades, terão grande importância no entendimento de como aplicar os filtros e também na compreensão de cada uma das funcionalidades apresentadas.

É importante ressaltar que o uso da ferramenta deve estar aliado a uma política de segurança da informação sólida dentro da empresa, já que esta constitui a fonte de todas as regras que serão transpostas para o **ASMG**. A mudança de cultura dos usuários internos também deve ser trabalhada, pois para proteger o ambiente corporativo, muitas restrições poderão ter que ser empregadas para garantir a eficiência da política de segurança adotada, resguardando o ambiente contra invasões, infecções e outras interferências.

De início é necessário conhecer a tela de administração das funcionalidades.

Figura 28. Janela acesso: Configuração do ASMG.

As opções de funcionabilidades estão divididas em grupos, sendo que cada uma trata de um assunto específico. Começando pelo item **"Configuração"**, será abordada cada uma das funcionalidades de forma detalhada, explicitando todos os

menus e telas envolvidas. Para tanto, criamos uma versão de demonstração do **ASMG** (demo_ASMG) que será utilizada como modelo para as explicações.

Configuração

O item **"Configuração"** agrega uma série de atributos que serão responsáveis pelo funcionamento geral da ferramenta. Os sub itens relacionados são os seguintes:

- Administração de Restrições;
- Gerenciamento de Administradores;
- Mensagens de Notificação;
- Servidor;
- SNMP;
- TCP/IP.

A seguir, será explicada cada uma das telas e funcionalidades envolvidas.

Administração de Restrições

Nesta janela é possível habilitar restrições de administração, ou seja, limitar as máquinas e/ou redes a partir de onde o servidor ASMG permitirá que alguém se conecte a ele através do Aker Control Center.

O comportamento padrão do sistema é permitir conexões remotas de qualquer origem. Para habilitar esta restrição, basta selecionar a opção **"Habilitar retrição de conexões"** e preencher a lista que aparece logo abaixo com as entidades do tipo Servidor e/ou Redes que for conveniente. Ao selecionar um servidor/rede para fazer parte da lista, será habilitada a possibilidade de administração remota a partir do (a) mesmo (a).

© Aker Security Solutions

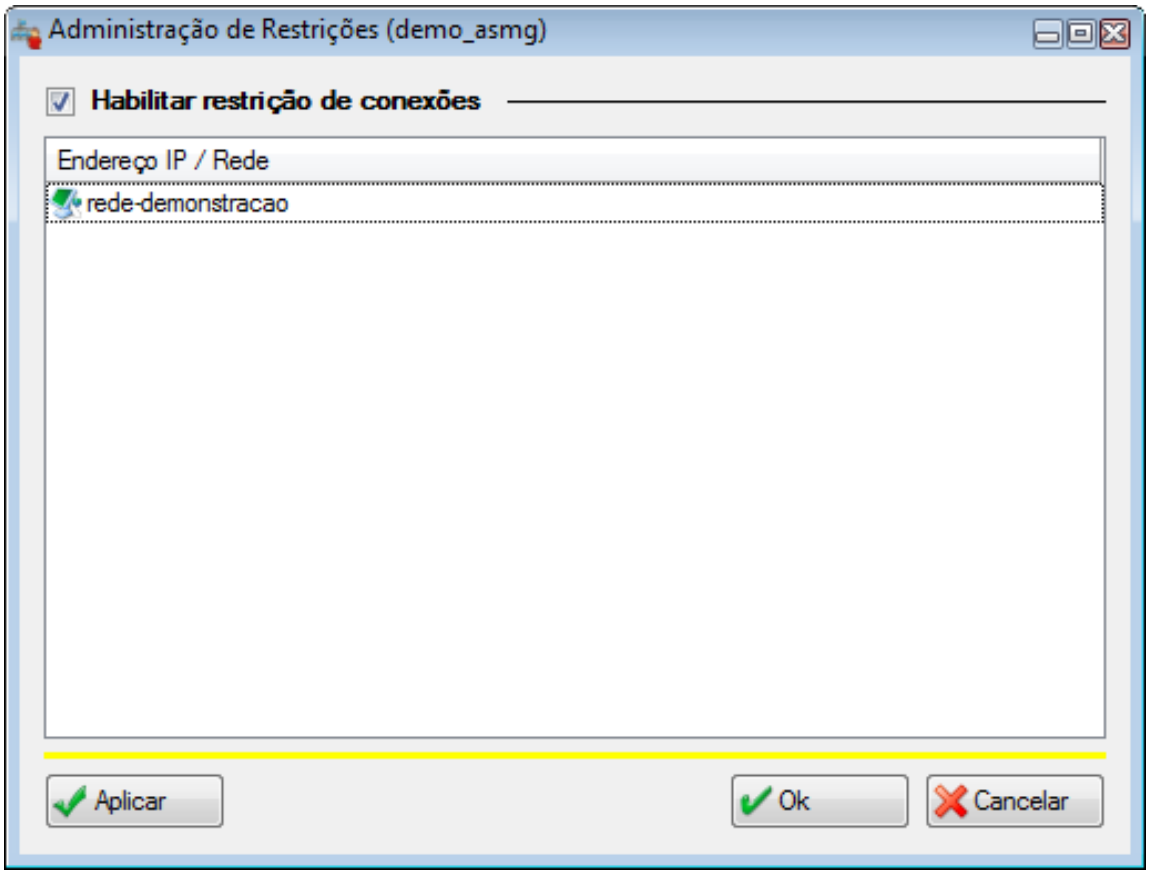

Figura 29. Administração de restrições de Endereço IP/Rede.

O preenchimento da lista de restrições só será possível caso já exista pelo menos uma entidade do tipo servidor ou rede.

Se, durante a configuração, o administrador não inserir uma entidade que inclua o seu IP atual, significa que ao desconectar do dispositivo remoto, não mais poderá se conectar ao ASMG desta mesma máquina. Para evitar problemas deste tipo, o sistema alerta o administrador sobre este fato sempre que puder ocorrer.

Gerenciamento de Administradores

Esta janela informa os nomes de todos os usuários do ASMG que podem ter acesso à interface de administração do sistema.

Para cadastrar um usuário, basta inserir seu login, nome, senha (não precisa ser igual à senha de rede) e confirmá-la em seguida. Nesta tela, ainda é possível excluir, adicionar e alterar informações de usuários.

É importante ressaltar que apenas usuários especialmente habilitados devem ser cadastrados como Administradores, tendo em vista que terão acesso a todas as outras configurações do sistema.

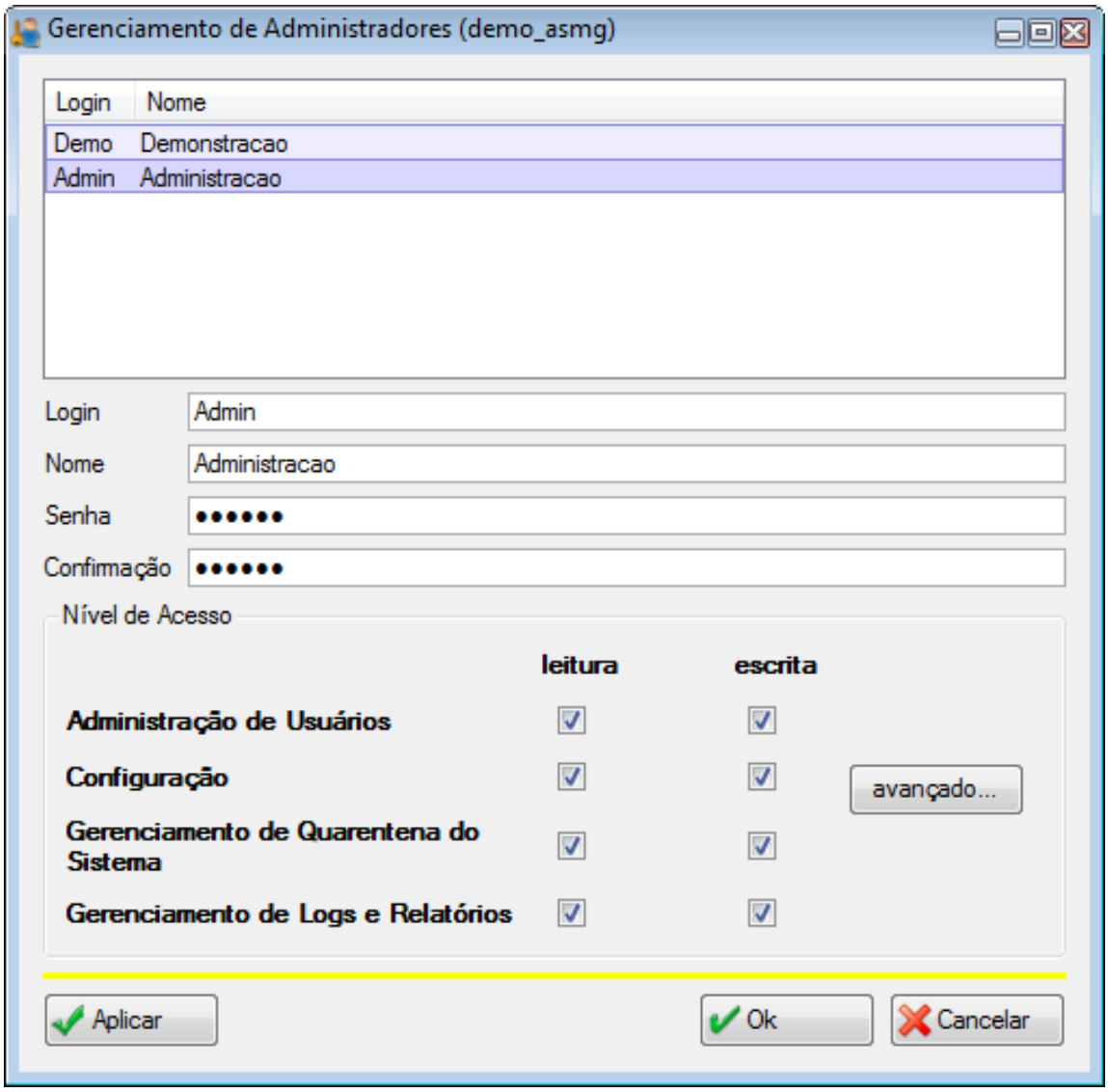

Figura 30. Gerenciamento dos Administradores.

O ASMG permite criar usuários com diferentes perfis e que terão acesso a diferentes funcionalidades da interface de administração, nas categorias de leitura e escrita. Tal fato permite que o administrador da rede relegue tarefas menos sofisticadas a outras pessoas de sua equipe, sem abrir espaço para que este(s) outro(s) usuário(s) possa(m) prejudicar o funcionamento do sistema.

Para o acesso de configuração, o ASMG oferece ainda opções avançadas de permissões, as quais possibilitam restringir o acesso em nível bastante granular. Por exemplo, é possível restringir o acesso de um usuário apenas para a leitura da configuração do repositório de sistema.

É possível criar e modificar usuários a partir de um binário de linha de comando no ASMG. Para tanto, basta utilizar o comando **/aker/bin/asmg/loginif**. Ao invocar o comando sem nenhum parâmetro, será apresentada uma lista completa de opções e sintaxe de uso. Note que por este procedimento todos os usuários criados serão administradores, ou seja, terão permissão total para a administração do sistema.

Mensagens de Notificação

O **ASMG** apresenta diversos tipos de filtros de anexos, que oferecem a opção de remoção do anexo original de acordo com parâmetros previamente definidos. Assim, determinados anexos podem ser removidos antes que a mensagem chegue ao seu destino.

Para cada situação onde ocorre a remoção do anexo, o Administrador pode especificar um texto para ser colocado em seu lugar, a fim de que a pessoa que receba a mensagem esteja ciente de que ali havia um anexo que foi removido, além do motivo desta remoção.

O texto a ser digitado é livre e é possível referenciar parâmetros como o nome do anexo que foi removido, o tipo do anexo ou o vírus que havia contaminado o anexo. Também é possível colocar mensagens já padronizadas do sistema, com versões em português e inglês, através do botão **"Aplicar Padrões"**.

Abaixo, segue a mensagem padrão utilizada em cada uma das situações onde os anexos são removidos.

© Aker Security Solutions

Remoção de Vírus

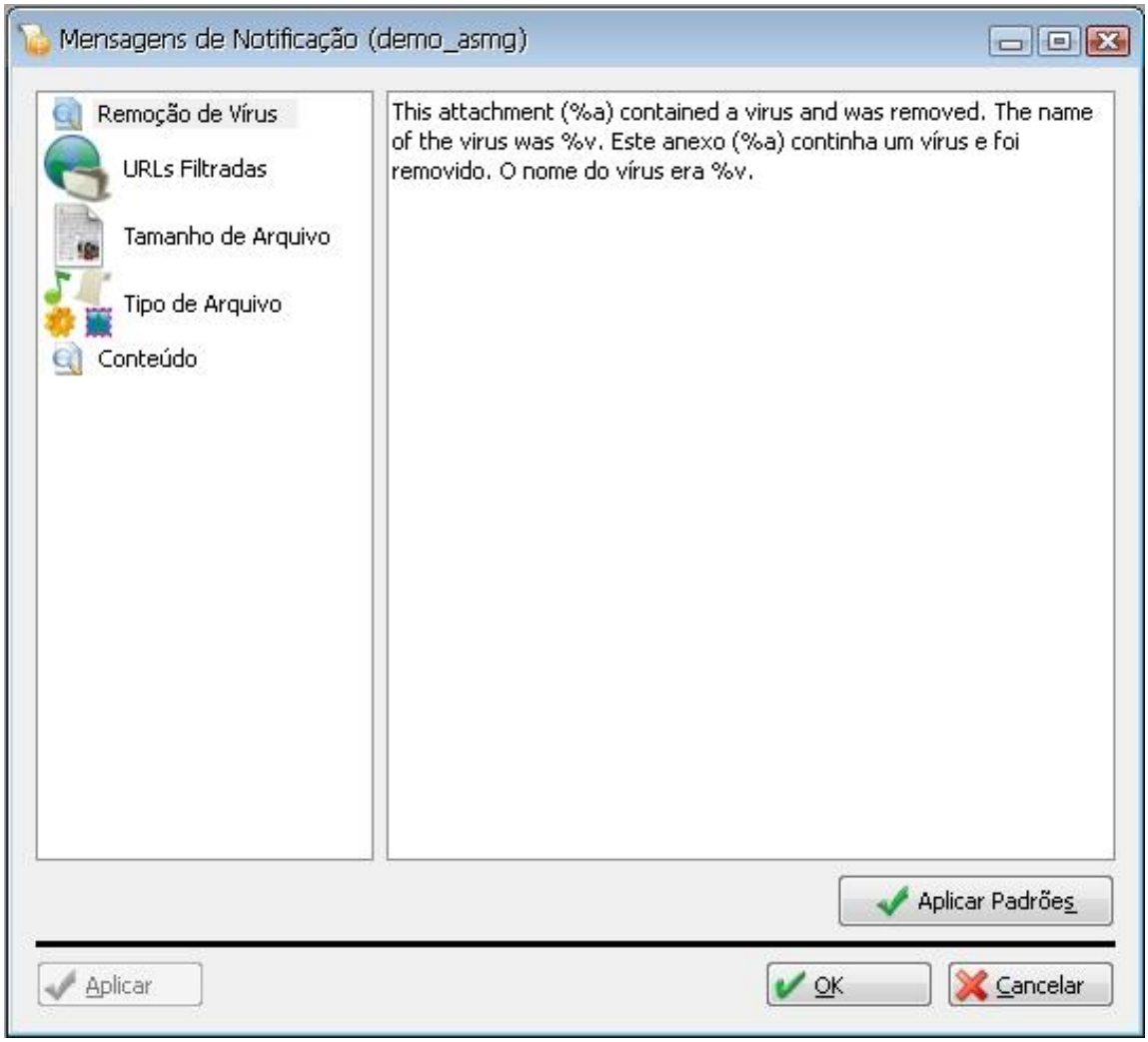
Mensagens de Notificação (demo_asmg)
Remoção de Vírus
URLs Filtradas
Tamanho de Arquivo
Tipo de Arquivo
Conteúdo
This attachment (%a) contained a virus and was removed. The name of the virus was %v. Este anexo (%a) continha um vírus e foi removido. O nome do vírus era %v.
Aplicar Padrões
Aplicar
OK
Cancelar

Figura 31. Mensagem de notificação – remoção de vírus.

URLs Filtradas

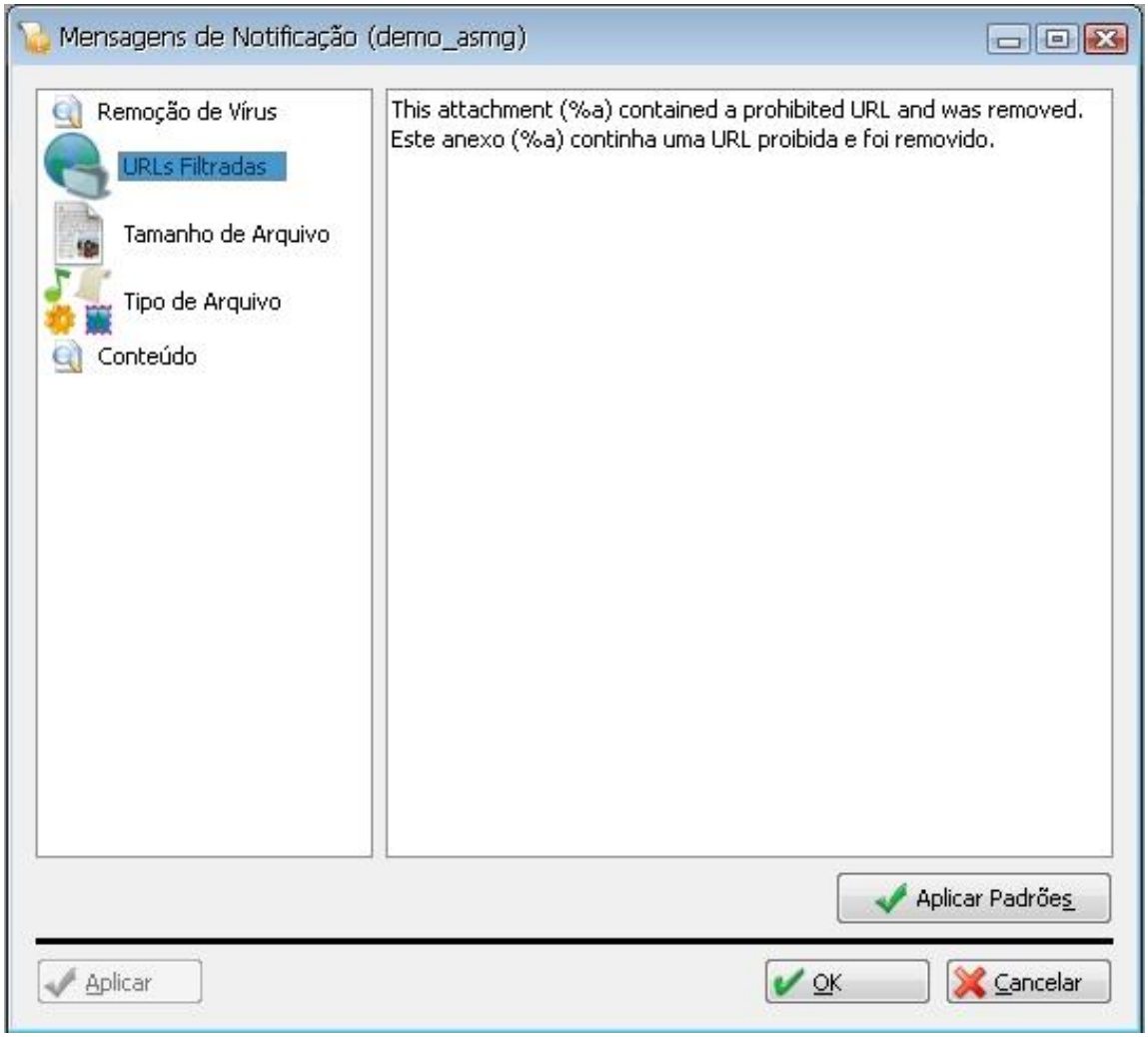

Figura 32. Mensagem de notificação – URL's filtradas.

Tamanho de Arquivo

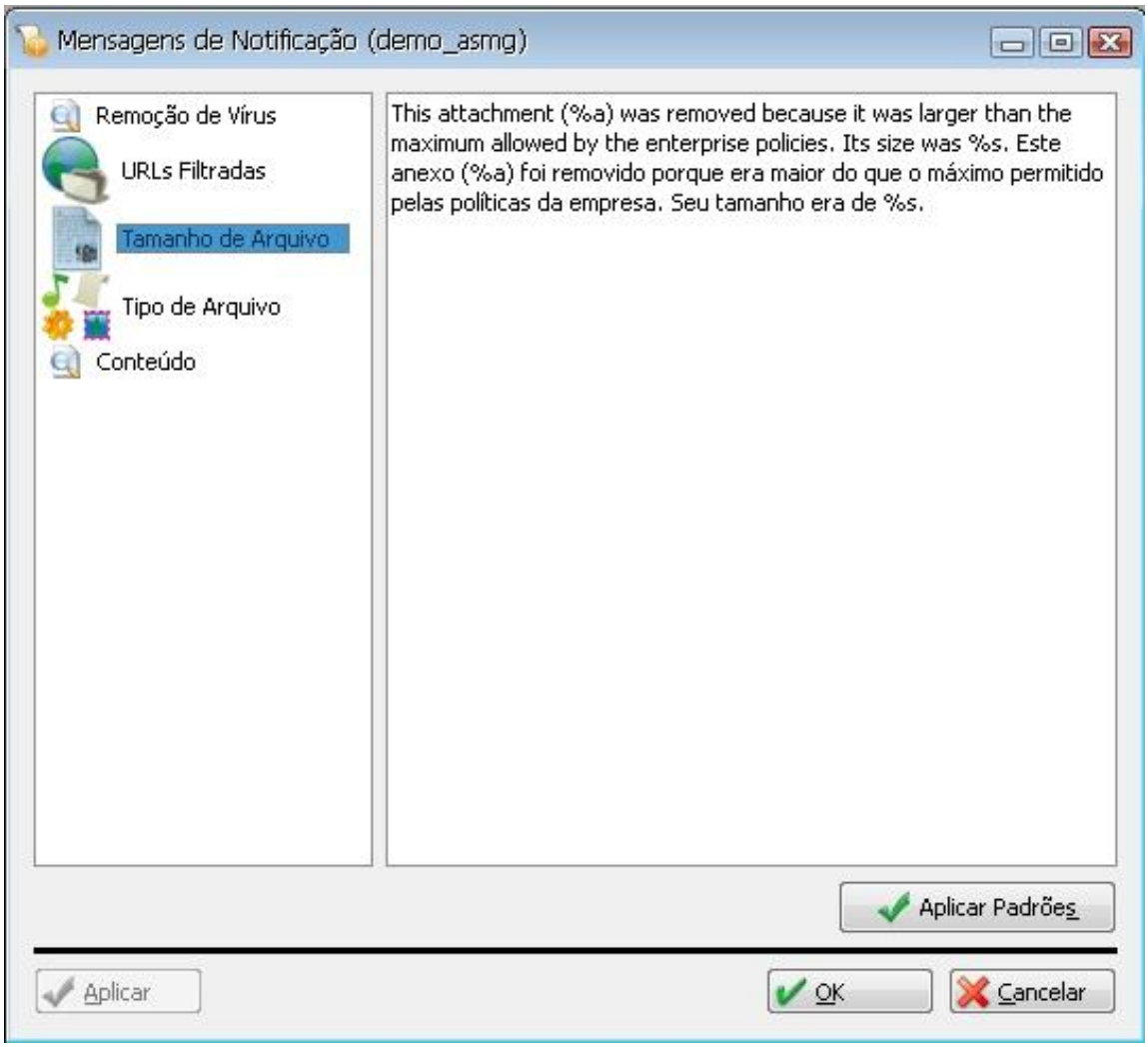
Mensagens de Notificação (demo_asmg)
Remoção de Vírus
URLs Filtradas
Tamanho de Arquivo
Tipo de Arquivo
Conteúdo
This attachment (%a) was removed because it was larger than the maximum allowed by the enterprise policies. Its size was %s. Este anexo (%a) foi removido porque era maior do que o máximo permitido pelas políticas da empresa. Seu tamanho era de %s.
Aplicar Padrões
Aplicar
OK
Cancelar

Figura 33. Mensagem de notificação – tamanho do arquivo.

Tipo de Arquivo

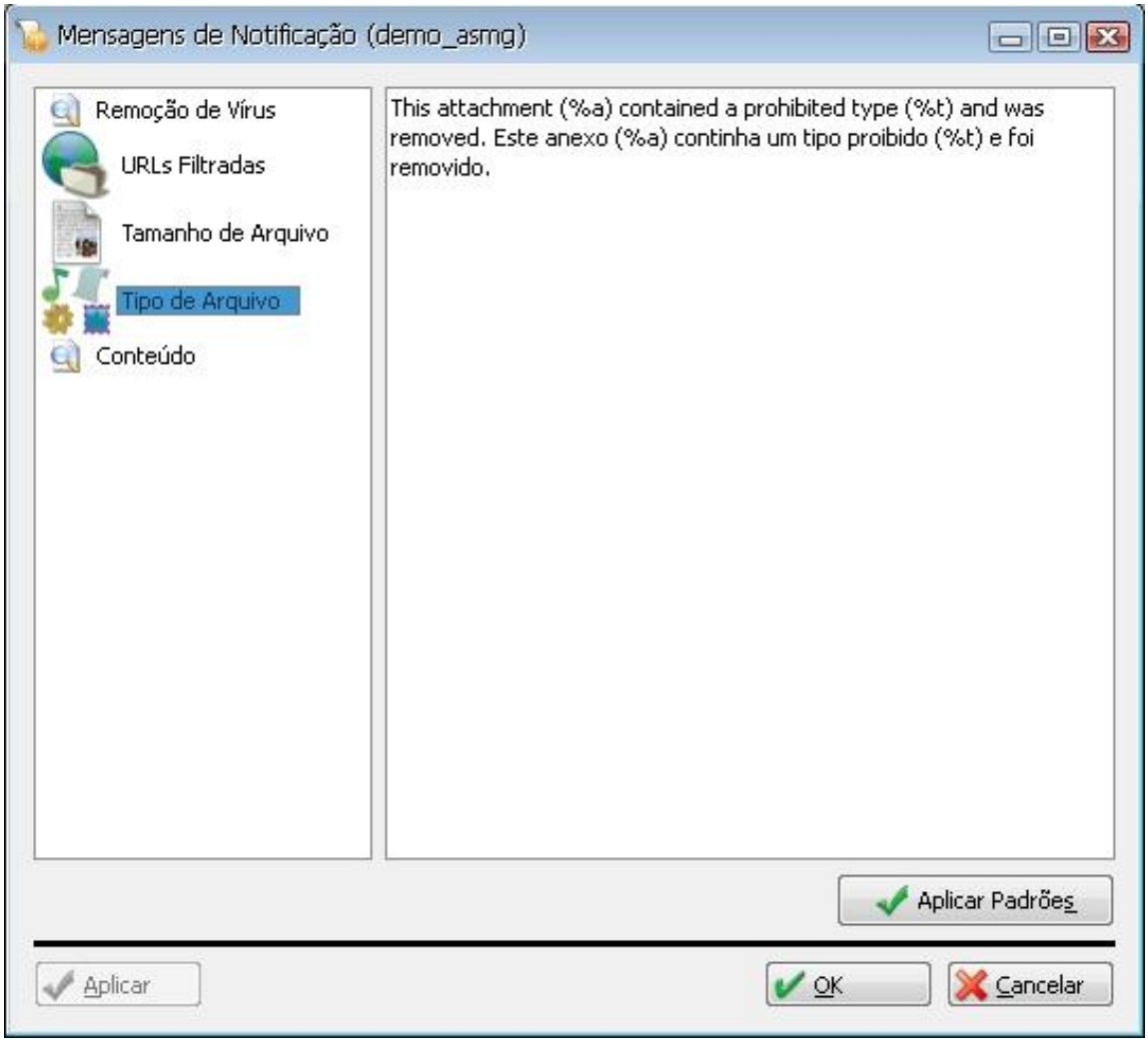

Figura 34. Mensagem de notificação – tipo de arquivo.

Conteúdo

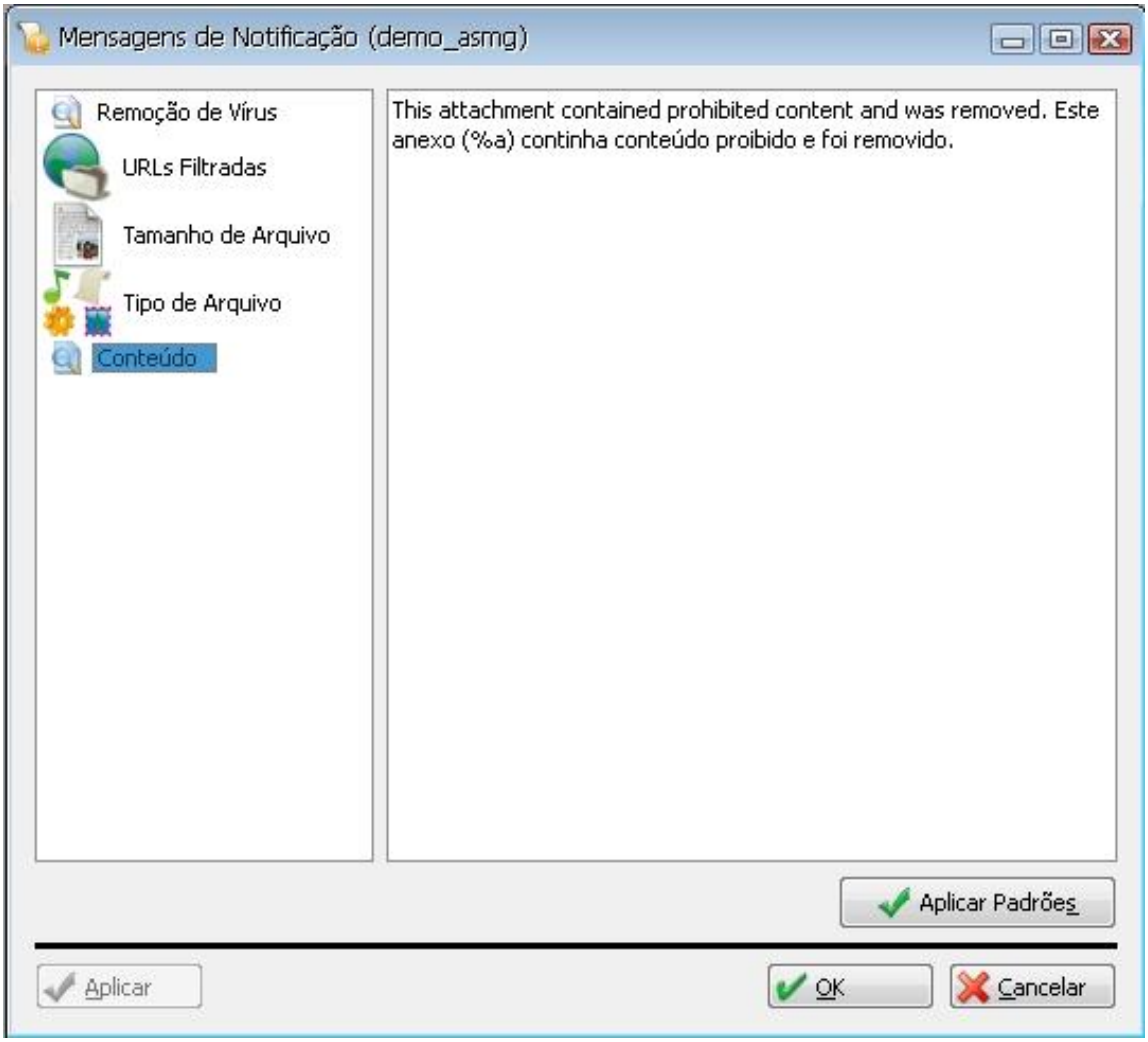

Figura 35. Mensagem de notificação – conteúdo.

Conforme verificado nas telas anteriores, existem alguns caracteres chamados "curingas", pois são substituídos por uma expressão dinâmica que se refere ao anexo removido. Estes curingas são, na verdade, ponteiros que armazenam o valor a ser assumido quando a mensagem for processada. Os possíveis caracteres curingas são:

- **%a:** usado para referenciar o nome do anexo original que foi removido;
- **%s:** usado para referenciar o tamanho do anexo original que foi removido;
- **%t:** usado para referenciar o tipo do anexo original que foi removido;
- **%v:** usado para referenciar o nome do vírus que havia no anexo original o qual foi removido.

© Aker Security Solutions

6..1. Servidor

Esta janela é uma das mais importantes e incorpora todos os parâmetros referentes aos protocolos SMTP e ESMTP, além de detalhes de conexão, e uso de arquivos temporários. Está dividida em diversas abas:

Aba Limites de Tempo

Nesta aba configuram-se os tempos-limite para as negociações de mensagens. A recomendação da RFC oficial do protocolo SMTP determina certos valores mínimos de tempo de espera, que podem ser obtidos quando clicados sobre o botão **"Aplicar Padrão"**. Estes tempos podem ser alterados, se for do interesse do Administrador, mas esta não é uma prática recomendável já que alguns servidores intermediários na transação podem estar muito ocupados e, por isso, demorar a responder a uma requisição. Na prática, isto pode significar atrasos na entrega ou várias tentativas de conexão na tentativa de concluir uma operação.

Quando um servidor A estabelece a comunicação com o servidor B para envio de mensagens, dizemos que o servidor A é cliente do servidor B. Já quando o servidor B estabelece conexão para envio de mensagens para A, dizemos que B é cliente de A. Outros termos que serão utilizados nas próximas linhas são: emissor (cliente) e receptor (servidor).

O **ASMG** pode agir tanto como servidor quanto cliente. A diferenciação dos papéis ocorre pelo tipo de tarefa que ele executa: ao estabelecer uma conexão com outro servidor para enviar uma mensagem, age como cliente; já quando recebe uma conexão de outro servidor para repassar as mensagens para os usuários internos, age como servidor.

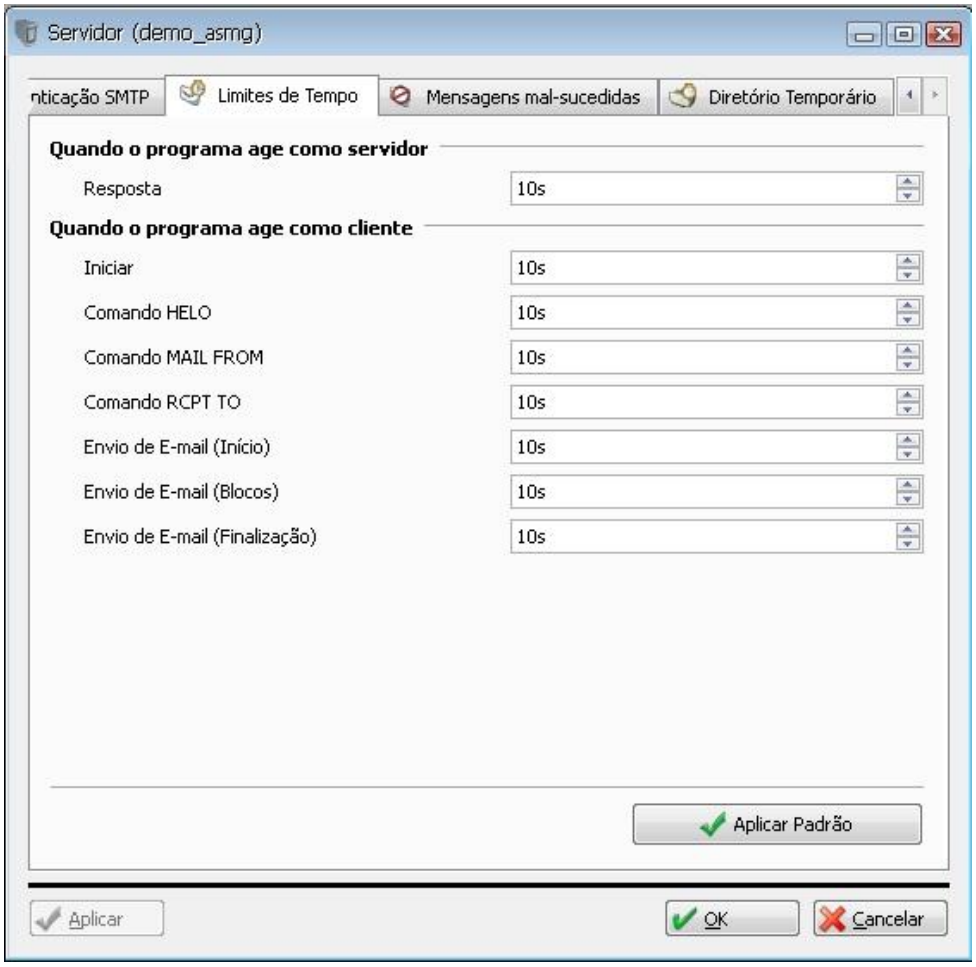

Figura 36. Servidor – limites de tempo.

Para melhor entendimento das opções existentes nesta aba, segue uma explicação para cada um dos valores mencionados:

- **Iniciar:** trata do tempo máximo de espera que o cliente tem para distinguir entre uma conexão TCP, falha e um atraso na espera de uma resposta positiva de conexão;
- **HELO:** mensagem obrigatória para início das negociações. Ela identifica para o receptor quem é o emissor. Se o emissor utilizar o protocolo ESMTP, é enviada a mensagem EHLO ao invés de HELO. Se o receptor possuir o suporte necessário, a mensagem não é recusada. Caso contrário, o protocolo utilizado será o SMTP;
- **MAIL FROM:** este comando designa quem é o remetente da mensagem;
- **RCPT TO:** este comando informa ao receptor o endereço do destinatário da mensagem. Caso o endereço não exista, a mensagem é recusada. Se houver múltiplos destinatários no mesmo domínio, este comando será repetido várias vezes;
- **Envio de E-mail (Início):** trata do tempo máximo de espera para que o cliente comece as transmissões após um comando indicando que iniciará o envio de dados;

- **Envio de E-mail (Blocos):** tempo limite para que o cliente aguarde que uma operação de envio de um bloco de dados seja concluída;
- **Envio de E-mail (Finalização):** tempo máximo para conclusão da operação.

6..2. Aba Recebendo E-mails

Esta aba é dedicada à configuração de parâmetros relativos ao recebimento de e-mails pelo **ASMG**.

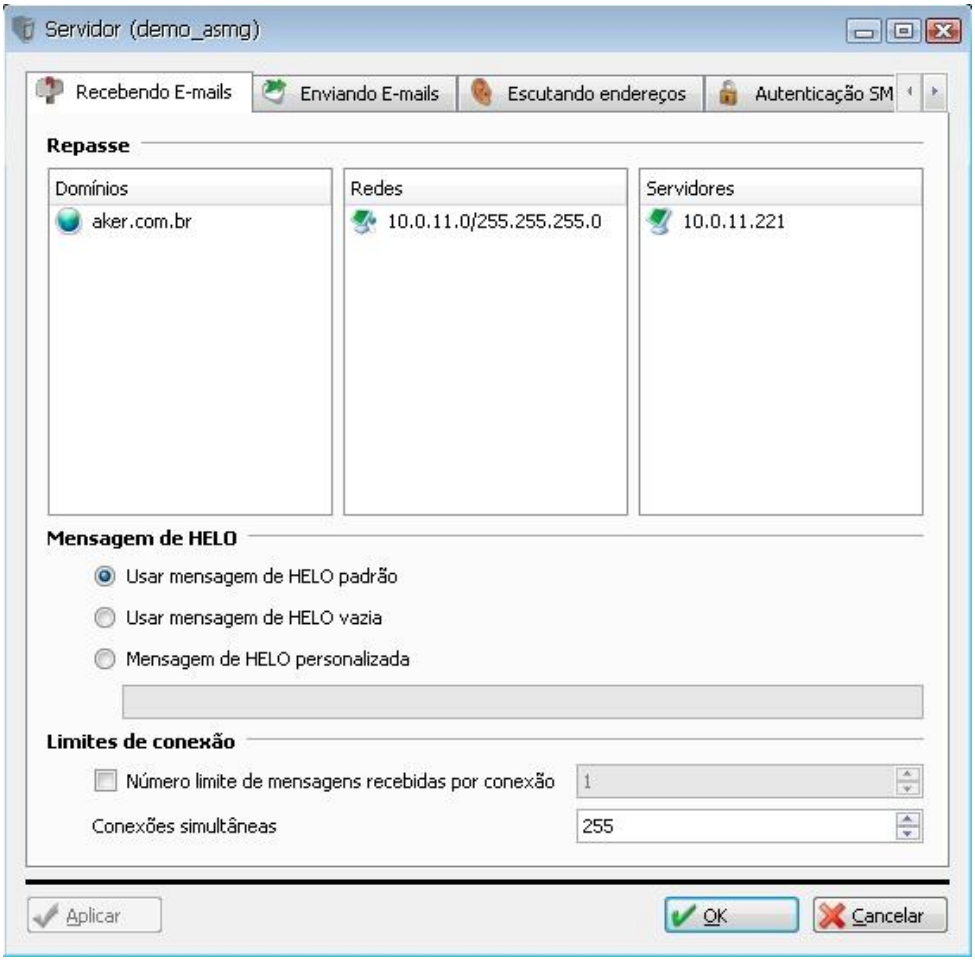

Figura 37. Servidor – recebendo e-mails.

O repasse de mensagens pode ser bloqueado ou liberado através do domínio, rede ou endereço do servidor remoto que a negocia ou, a partir do domínio que ela se destina.

Conforme mostrado na **acima**, a tela está dividida em três subseções:

Repasse

No exemplo acima, pode-se ver que há duas entidades do tipo **"Domínio"** referenciadas no campo de mesmo nome. Isto quer dizer que quaisquer mensagens

interceptadas pelo **ASMG** e que sejam direcionadas aos domínios *seudominio.com.br* ou *meudominio.com.br* terão seus repasses, ou *relay*, garantidos. Neste caso, também significa que qualquer servidor que pertença a um desses domínios terá suas mensagens repassadas, para qualquer domínio desejado. O mesmo aconteceria com as entidades do tipo **"Redes"** e do tipo **"Servidores"** que estivessem instanciadas em seus respectivos campos.

Para instanciar uma entidade, basta seguir os passos abaixo (tomando como exemplo o campo Redes):

- Clicar com o botão direito do mouse sobre a tela **"Redes"**;
- Clicar sobre a opção **"Adicionar identidade"**;
- Selecionar a entidade do tipo **"Rede"** desejada e clicar em **"Adicionar"**.
- Para instanciar mais de uma entidade, basta repetir os passos de 1 a 3.

Mensagem de HELO

Exitem 3 opções: usar a mensagem padrão, não utilizar nenhuma mensagem ou então usar uma mensagem personalizada. Basta selecionar a opção desejada e, caso opte por uma mensagem personalizada, ao marcar esta opção, a caixa de texto ficará livre para edição.

Limites de Conexão

Nesta tela determina-se a quantidade máxima de mensagens que serão recebidas por conexão, além de limitar as conexões simultâneas ao servidor. Podem ser alterados de acordo com o critério adotado pela política de segurança da empresa.

6..3. Aba Enviando E-mails

Esta aba é dedicada às questões relativas ao envio de mensagens.

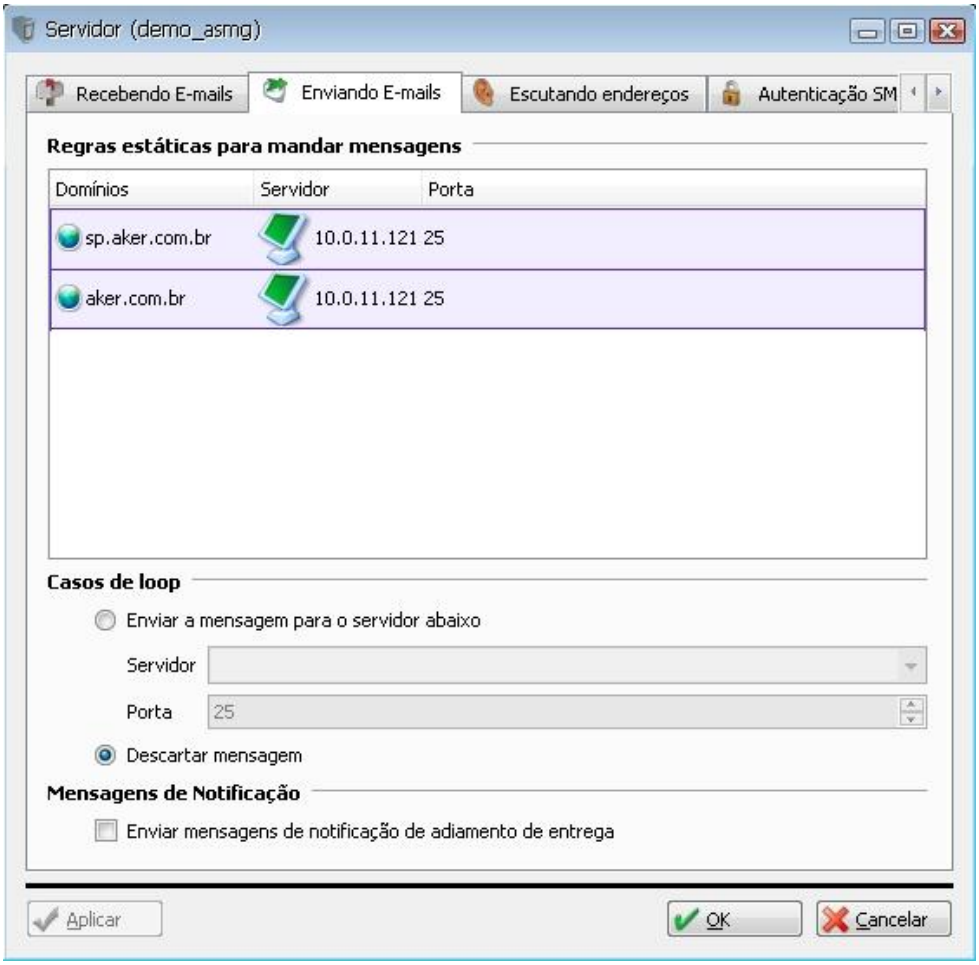

Figura 38. Servidor – enviando e-mails.

Regras estáticas para mandar mensagens

Se o domínio do destinatário estiver listado na janela **"Domínios"**, o **ASMG** utiliza o servidor correspondente para fazer a transação de repasse. Caso contrário, o produto realiza uma pesquisa DNS para descobrir qual o MX responsável por aquele domínio e, assim, poder encaminhar a mensagem.

Para adicionar uma nova regra clicar com o botão direito do mouse sobre o quadro de regras e escolher a opção **"Inserir"**. Aparecendo a linha a ser editada, clicar com o botão direito do mouse logo abaixo de **"Domínios"** e escolher a opção **"Adicionar Entidades"**. Pode ser selecionado mais de um domínio ao mesmo tempo, bastando manter a tecla **<SHIFT>** pressionada, enquanto realiza a escolha.

Especificar o servidor de envio, clicar com o botão direito do mouse no campo **"Servidor"**. Escolher a opção **"Adicionar Entidades"** e escolher o servidor dentro da relação já previamente cadastrada.

© Aker Security Solutions

Casos de loop

Caso seja detectado algum loop durante o envio, ou seja, uma mesma mensagem re-encaminhada ao **ASMG,** é possível informar um servidor para onde à mensagem deve ser encaminhada. Se desejar obter este efeito, marcar a opção **"Enviar a mensagem para o servidor abaixo"** e escolher um servidor dentre os já previamente cadastrados.

Também é possível escolher a opção **"Descartar a mensagem"** caso não deseje tratar o caso de loop.

Mensagens de notificação

Caso haja algum erro temporário no servidor remoto no envio de uma mensagem, pode-se marcar a opção **"Enviar mensagem de notificação de adiamento de entrega"** para que o **ASMG** construa e envie uma mensagem para o remetente original informando-o sobre o atraso na entrega.

Um erro temporário ocorre em situações diversas, como por exemplo, quando o servidor de destino não possui espaço em disco suficiente para receber a mensagem enviada a partir do **ASMG**, ou há uma falha de comunicação entre o emissor e o receptor. Significa algo como "tente novamente mais tarde".

Por padrão esta opção vem desabilitada. Caso seja necessário habilitá-la, basta marcar a caixa de verificação localizada à esquerda.

6..4. Aba Endereços de Escuta

O servidor de correio fica permanentemente escutando uma determinada porta à espera de conexões de outros servidores para o recebimento de mensagens. Assim que detecta uma conexão, inicia-se a negociação entre o cliente e o servidor para recepção das mensagens.

Para informar ao **ASMG** qual o endereço de escuta, clicar com o botão direito do mouse no quadro e escolher a opção **"Inserir"**. Aparecendo a linha a ser editada, clicar com o botão direito do mouse logo abaixo da coluna **"Endereço IP local"** e digitar o endereço desejado. Por padrão, o protocolo SMTP utiliza a porta 25, então ela já é selecionada automaticamente.

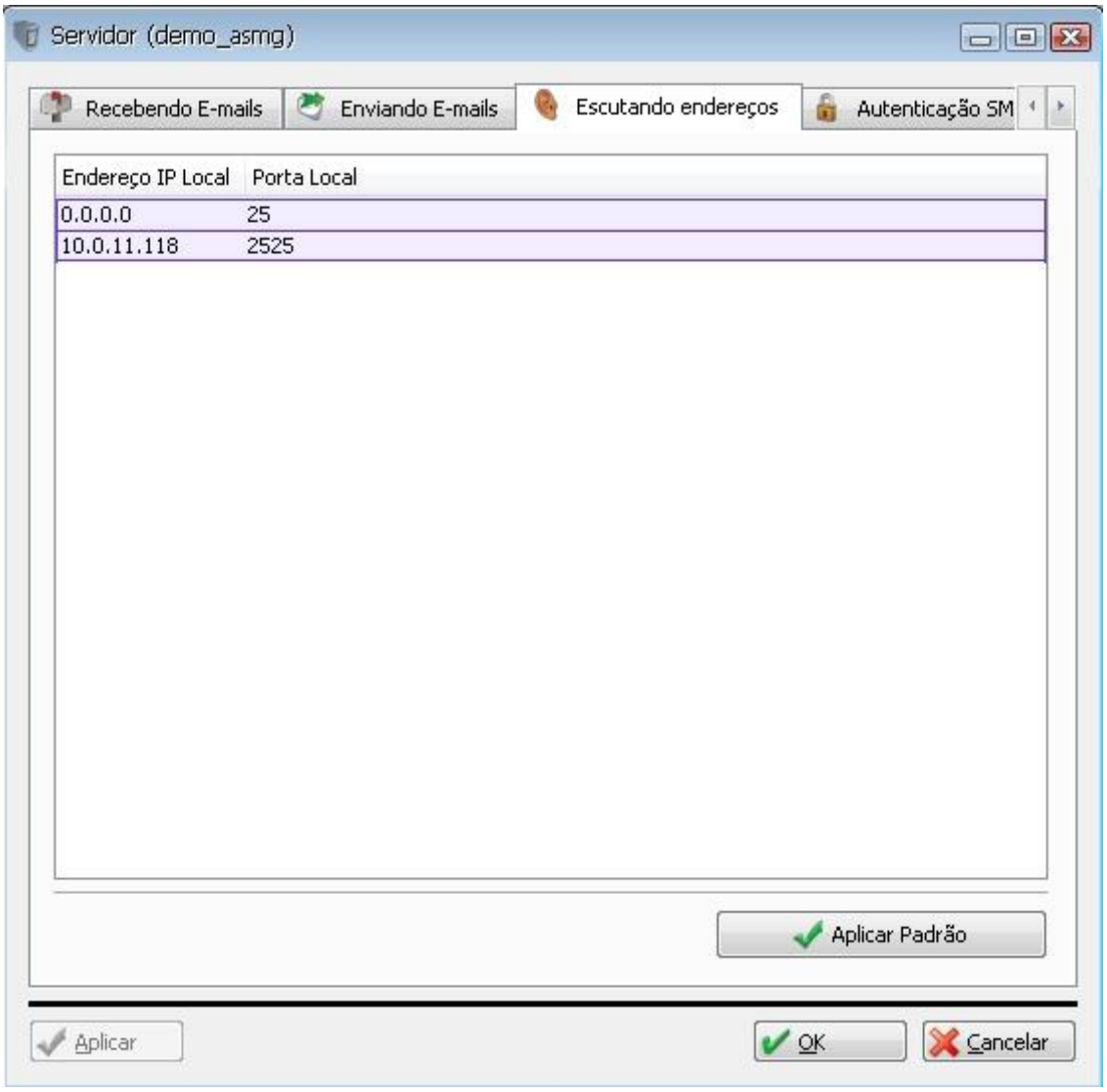

Figura 39. Servidor – endereços de escuta.

O botão **"Aplicar Padrão"** insere a notação "0.0.0.0", que significa que o **ASMG** deve ouvir todas as interfaces de rede do servidor.

6..5. Aba autenticação SMTP

Nesta aba configura-se a autenticação SMTP, que pode ser executada através dos métodos PLAIN (a senha do usuário é transmitida livremente sem nenhuma codificação) e LOGIN (a senha do usuário é apenas codificada em base-64). A consulta pode ser realizada em base de dados MySQL ou em autenticadores Aker cadastrados como entidades.

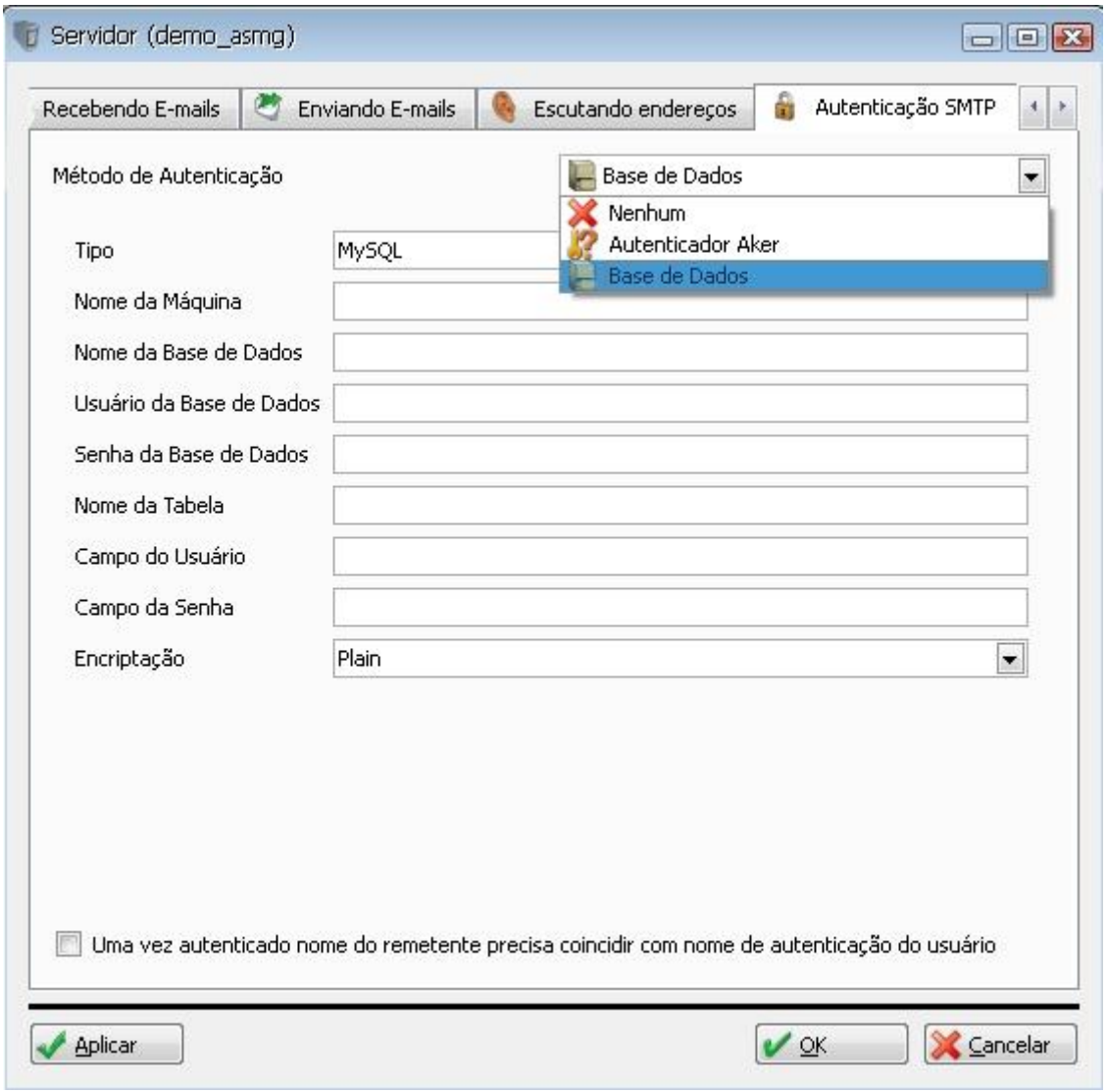

Figura 40. Servidor – autenticação SMTP.

Opcionalmente, o administrador pode ainda escolher que todas as mensagens de saída que sofram autenticação SMTP tenham que usar o mesmo usuário da autenticação para o remetente da mensagem. Isso impede que um usuário se passe por outro.

6..6. Aba Mensagens mal-sucedidas

Nesta aba e escolhido o diretório onde as mensagens que não conseguiram ser transmitidas devido a alguma má formatação ou erro temporário de comunicação com o servidor de destino, devem ser armazenadas. Segundo a RFC 2821, que trata dos padrões a serem adotados pelo protocolo SMTP, caso o emissor não consiga transmitir a mensagem logo na primeira vez, deve tentar retransmiti-la pelos próximos cinco dias. Caso isso não aconteça, o envio da mensagem é abortado e o remetente é avisado.

© Aker Security Solutions

Se o Administrador resolver armazenar estas mensagens, basta marcar a caixa **"Habilitar a armazenagem de mensagens mal-sucedidas"** e informar o local de armazenamento.

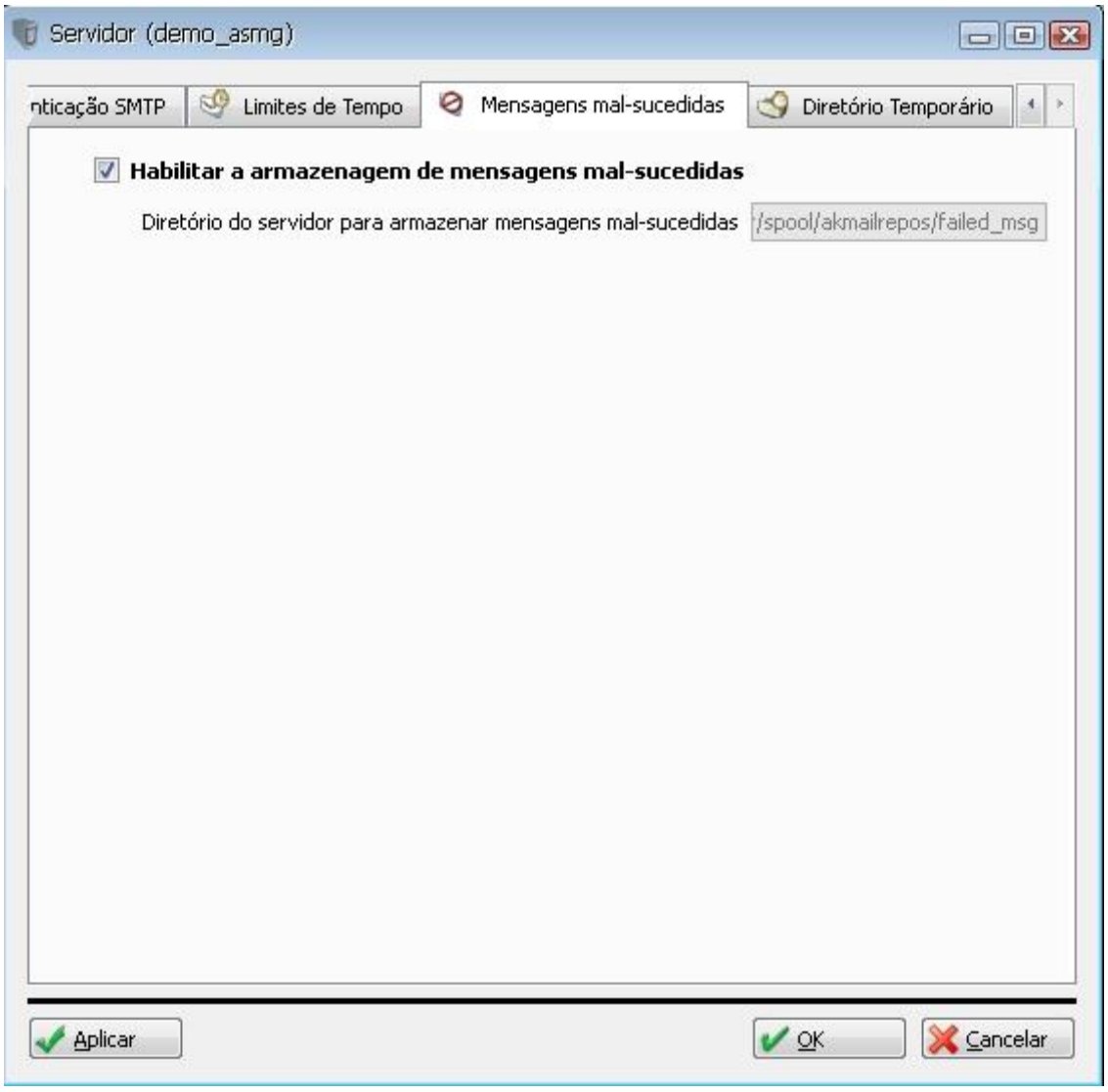

Figura 41. Servidor – mensagens mal sucedidas.

6..7. Aba Diretória Temporário

Nesta aba configura-se o diretório onde o **ASMG** deve armazenar informações temporárias, relativas às mensagens que estão sendo processadas. Basta informar o caminho completo do diretório na caixa **"Diretório Temporário"**.

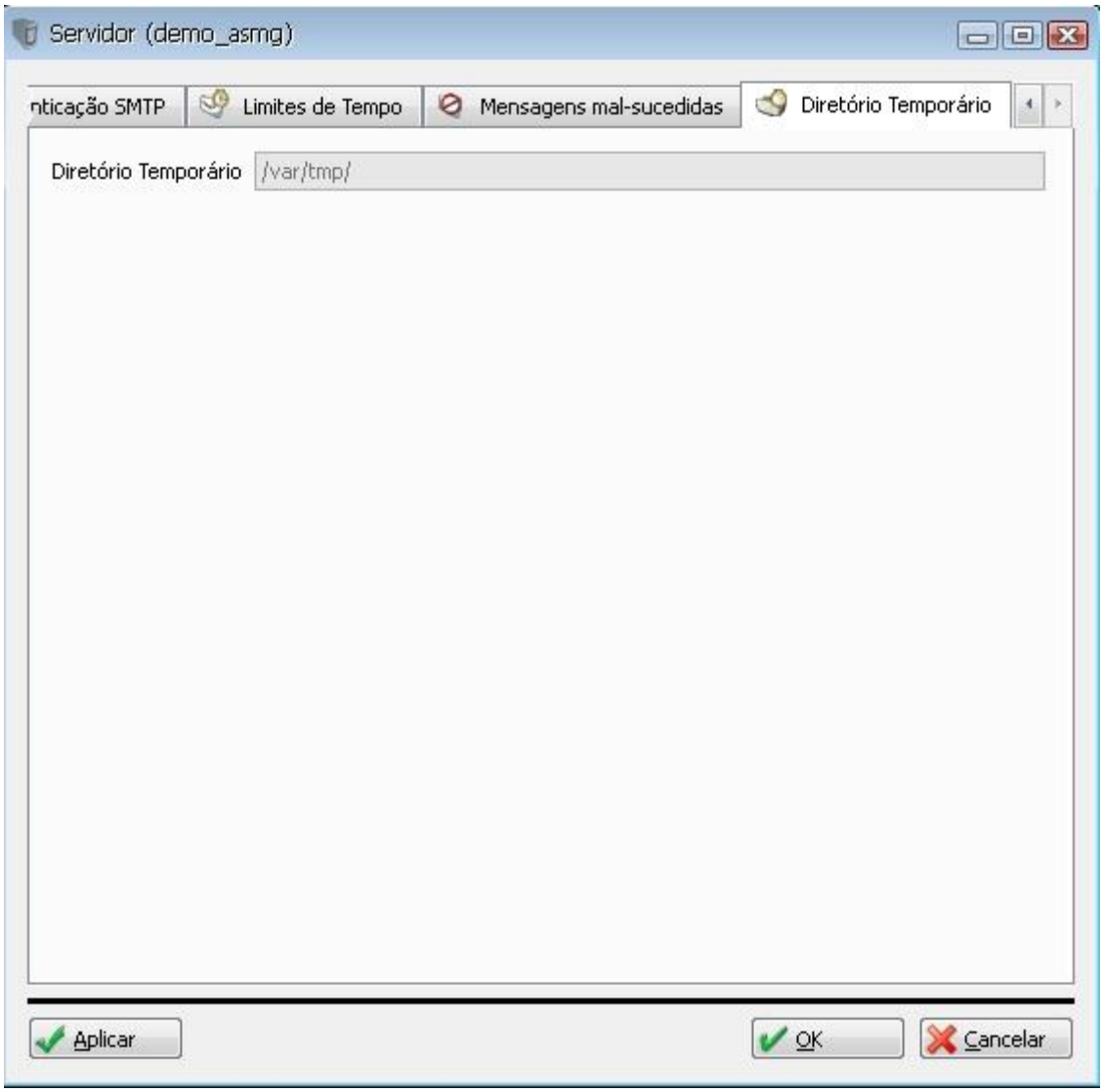

Figura 42. Servidor – diretório temporário.

6..8. Aba Whitelist e Blacklist

Nesta aba configura-se a ordem de consultas das whitelists e blacklists do ASMG, permitindo ao administrador definir as prioridades na consulta a estas listas, que podem conter:

- Listas de e-mails;
- Domínios;
- Listas de Domínios.

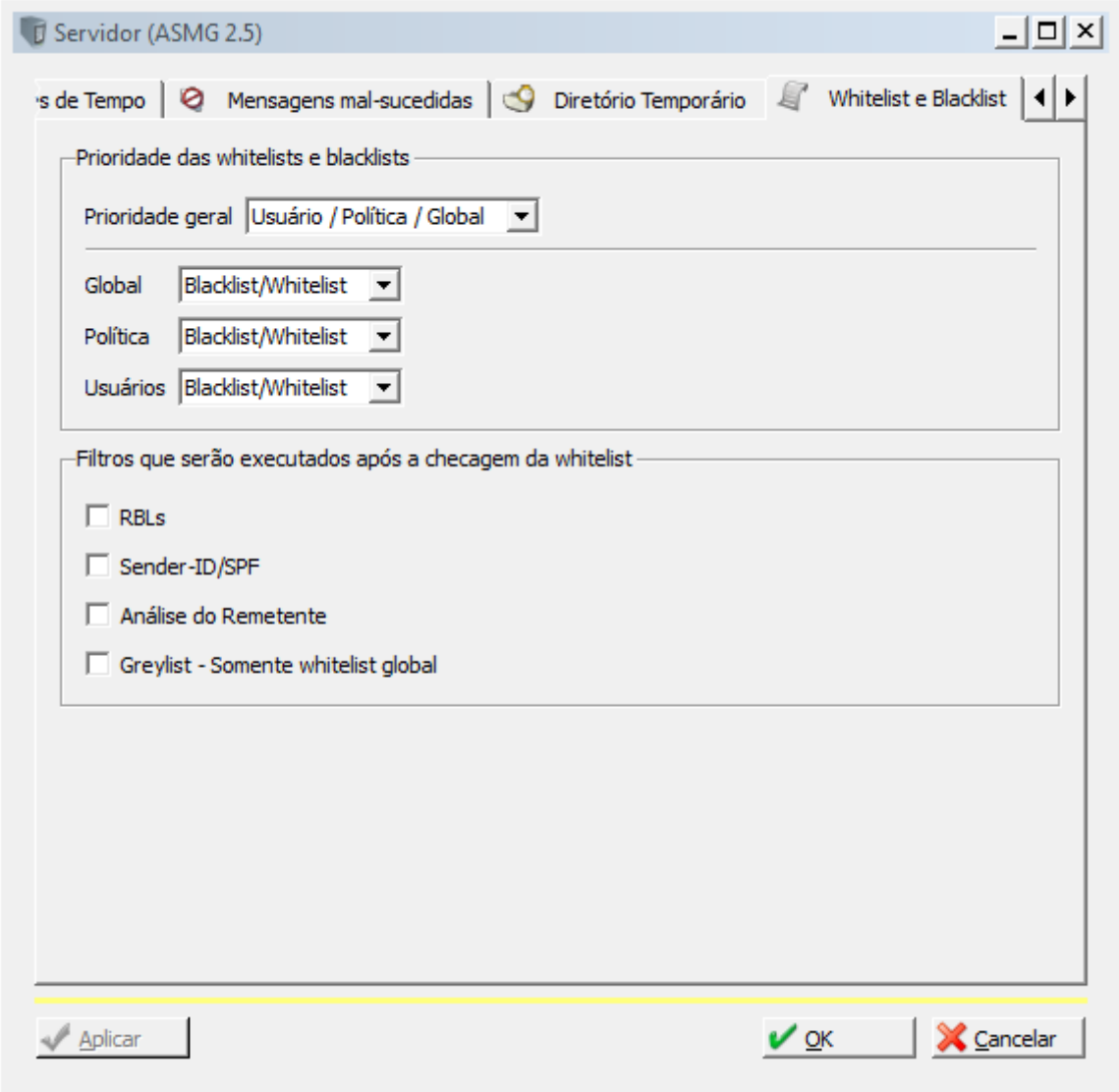

Figura 43. Servidor – whitelist e blacklist.

Entre as opções o administrador pode optar pelas seguintes ordens de consultas das listas:

- Prioridades das whitelists e blacklists:

  Prioridade geral – seguintes opções:

  - Usuário / Políticas / Global;
  - Global / Políticas / Usuários;
  - Global / Usuários / Políticas.

Internamente em cada uma das três listas o administrador pode definir qual será a ordem de consulta entre a whitelist e blacklist.

- Filtros que serão executados após a checagem da whitelist:

Os filtros selecionados abaixo serão executados somente após a checagem nas listas, conforme a prioridade definida nas opções anteriores, o administrador têm as seguintes opções:

- RBLs;
- Sender-IF/SPF;
- Análise de Remetente;
- Graylist – Somente whitelist Global.

6..9. Aba Watch Dog

Nesta aba configuram-se as ações do ASMG em caso de receber de mensagens com problemas de formatação (parser) e o tempo máximo para processamento de uma mensagem.

Estas ações são realizadas para termos um tratamento automático de travamentos de fila de e-mails e evitar o aumento excessivo destas filas durante seu processamento.

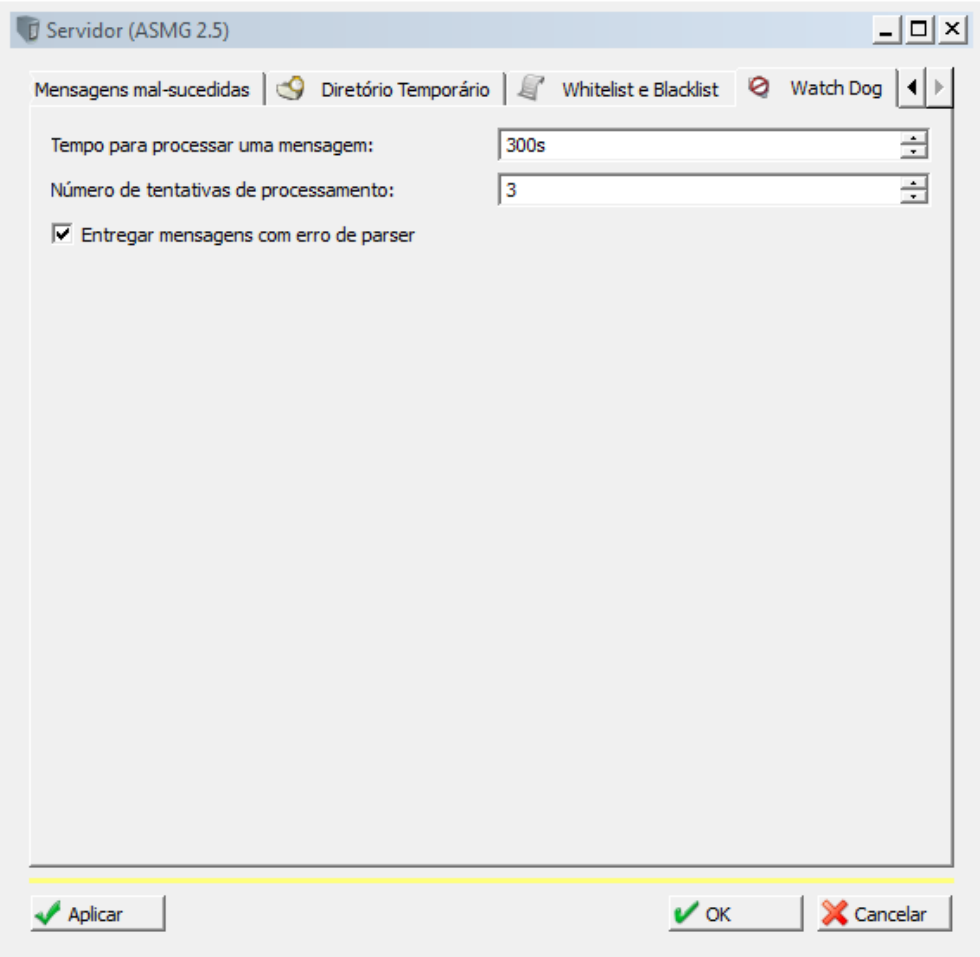

Figura 44. Servidor – watch dog.

Entre as opções o administrador pode configurar:

- Tempo para processar uma mensagem – define o tempo máximo que o sistema pode processar uma mesma mensagem, caso este tempo seja excedido o sistema será reiniciado (processo engine) e à mensagem será descartada;
- Número de tentativas de processamento – define o número máximo de tentativas de processar uma mesma mensagem que travou o sistema, depois de excedido o número de tentativas a mensagem é descartada;
- Entregar mensagens com erro de parser – ativando esta opção mensagens com problemas de formatação são liberadas sem passar pelos filtros da Política (veja capítulo "**Políticas**").

SNMP

Esta janela permite configurar os parâmetros do protocolo SNMP, utilizado para monitorar várias informações como processamento da máquina, uso de memória, tráfego na rede, etc.

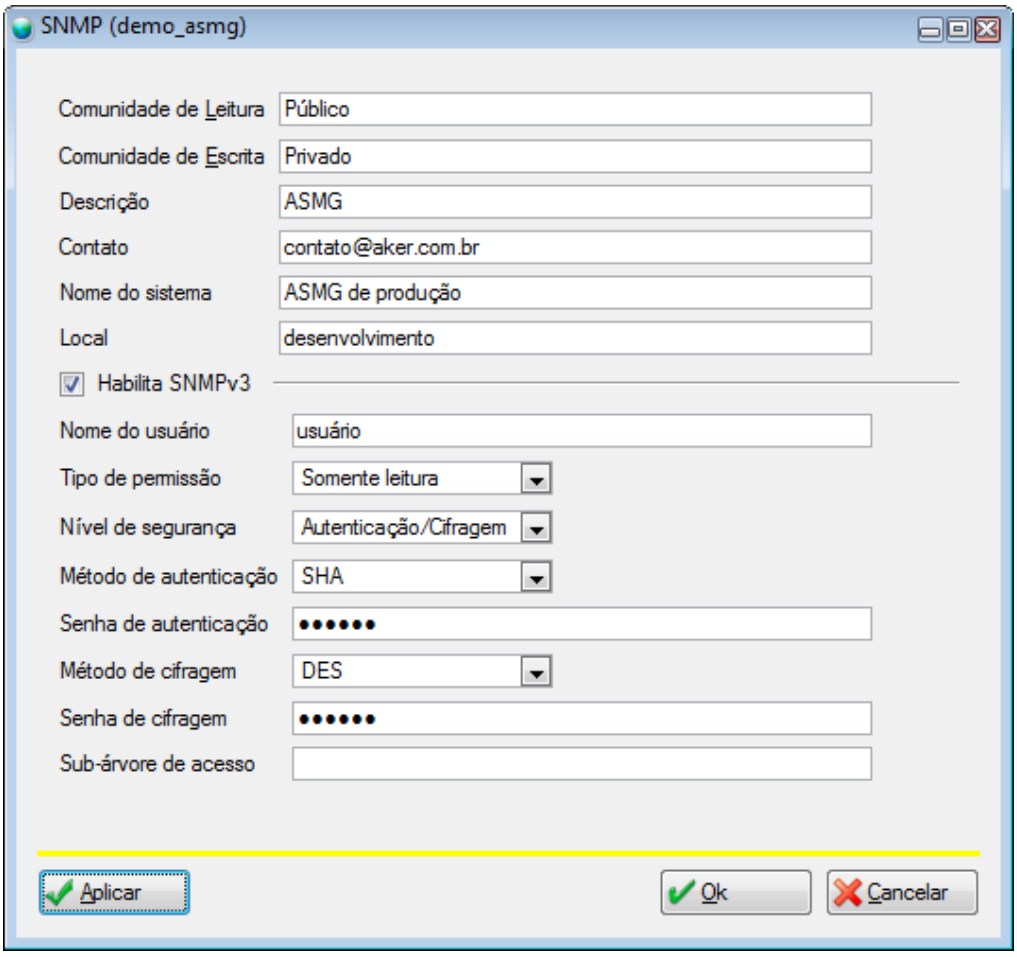

Figura 45. Configuração dos paramentros do protocolo SNMP.

Comunidade de leitura: Este parâmetro indica o nome da comunidade que está autorizada a ler dados do ASMG via SNMP. Caso este campo esteja em branco, nenhuma máquina estará autorizada a lê-los.

Valor padrão: ***campo em branco***

Comunidade de escrita: Este parâmetro indica o nome da comunidade que está autorizada a alterar dados do ASMG via SNMP. Caso este campo esteja em branco, nenhuma máquina estará autorizada a alterá-los.

Valor padrão: ***campo em branco***

Mesmo com uma comunidade de escrita definida, por razões de segurança, somente poderão ser alterados algumas variáveis do grupo ***system***.

Descrição: Tipo de serviço que a máquina disponibiliza para o usuário;

Contato: Tipo de contato (e-mail, home page) que o administrador disponibiliza para o usuário;

Nome: Nome abreviado do sistema que o identifica na rede, ex: DNS;

Local: Local físico onde a máquina está instalada.

O SNMPv3 inclui três importantes serviços: autenticação (authentication), privacidade (privacy) e controle de acesso (access control).

Habilita SNMPv3: Ao selecionar essa opção permite definir o tipo de permissão de um usuário e qual o nível de segurança que ele estará relacionado.

Nome do usuário: Nome do usuário que terá permissão para conferir ou modificar as informações.

Tipo de permissão: Permite a escolha do tipo de permissão do usuário. Poderá ter acesso de somente leitura dos dados ou de leitura e escrita.

Nível de segurança: Permite a escolha do tipo de segurança dos dados. Pode-se optar por nenhuma autenticação, com autenticação ou autenticação com cifragem. Caso a escolha seja com autenticação, as opções **"Método de autenticação"** e **"Senha de autenticação"** serão habilitadas. Caso a escolha seja autenticação com cifragem, as opções **"Método de cifragem"** e **"Senha de cifragem"** serão habilitadas.

Método de autenticação: Possuem dois métodos de autenticação, um com o algoritmo MD5 e o outro com o algoritmo SHA.

Senha de autenticação: Deve ser informada uma senha para autenticação, com no mínimo 8 caracteres.

Método de encriptação: Possuem dois métodos de cifragem dos dados, um por meio do algoritmo DES e o outro por meio do algoritmo AES.

Senha de encriptação: Deve ser informada uma senha para cifragem, com no mínimo 8 caracteres.

Ramo de acesso: Permite restringir, por meio de sub-árvores, quais os grupos de dados/informações que o usuário terá acesso.

TCP/IP

Esta opção permite configurar todos os parâmetros de TCP/IP do ASMG através da interface gráfica. É possível configurar os endereços de interfaces de rede, DNS e rotas.

Para ter acesso à janela de configuração TCP/IP deve-se:

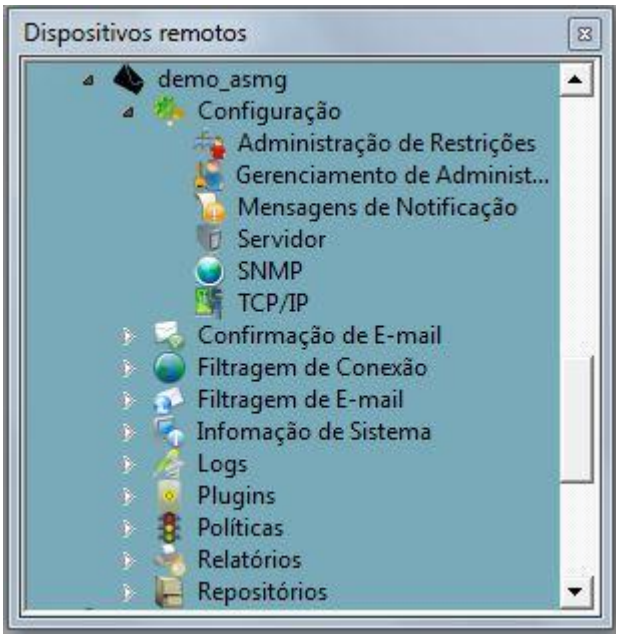

Figura 46. Aba de acesso: configuração TCP/IP.

- Clicar no menu *Configurações do Sistema* da janela de administração do ASMG;
- Selecionar o item *TCP/IP*.

A janela de configuração TCP/IP

Esta janela consiste de três pastas onde cada uma é responsável por um tipo de configuração diferente. São elas:

Aba de DNS

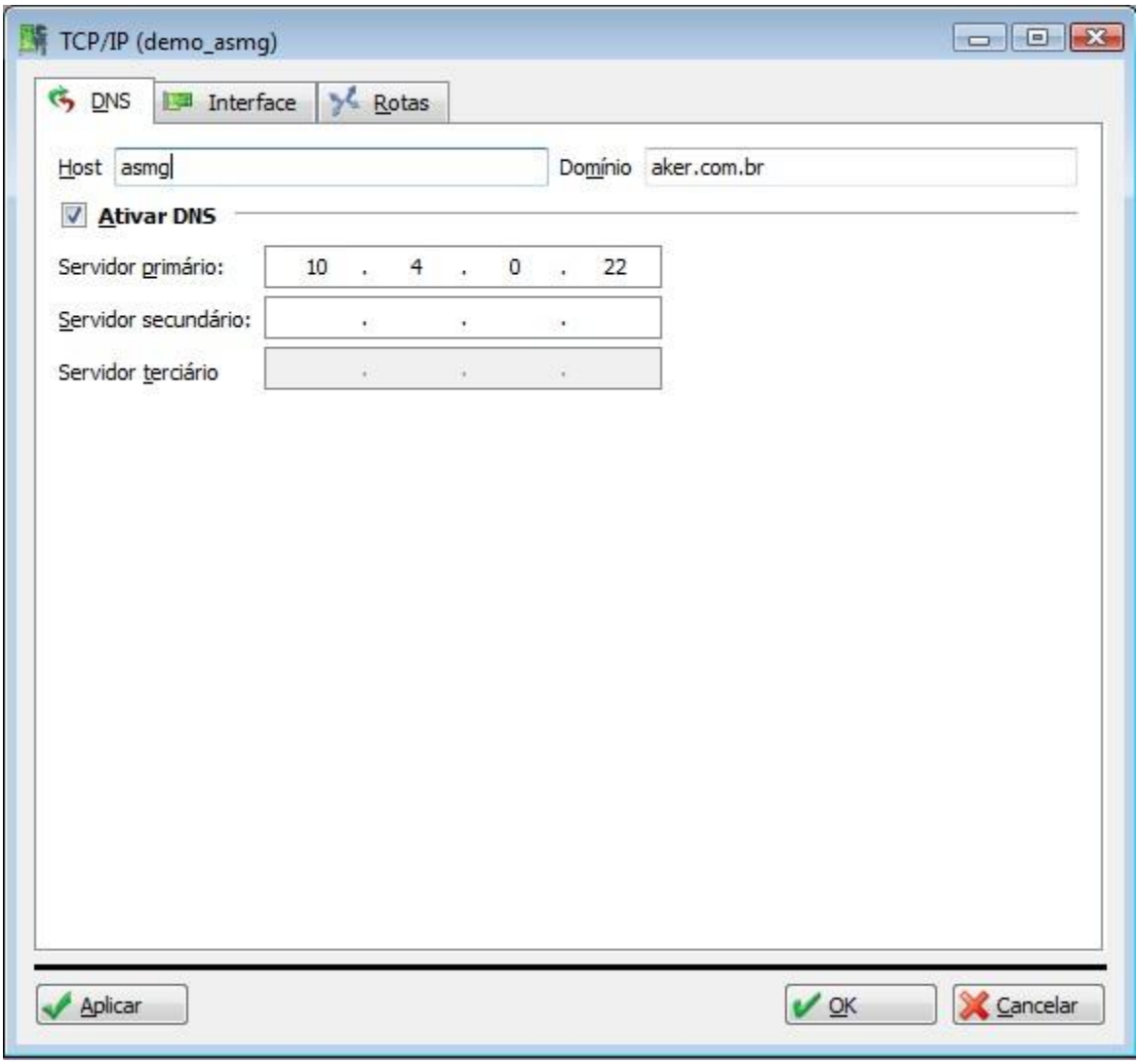

Figura 47. TCP/IP - DNS.

Nesta pasta são configuradas todas as opções relacionadas com a resolução de nomes ou DNS. Ela consiste dos seguintes campos:

Máquina: Nome da máquina na qual o ASMG está rodando.

Domínio: Nome do domínio no qual o ASMG está rodando.

Ativar DNS: Esta opção deve ser marcada para ativar a resolução de nomes via DNS e desmarcada para desativá-la.

Servidor primário: Definir o servidor DNS primário que será consultado para se resolver um nome. Ele é obrigatório se a opção *DNS ativo* estiver marcada.

Servidor secundário: Definir o servidor DNS secundário que será consultado se o primário estiver fora do ar. Ele é opcional.

Servidor terciário: Definir o servidor DNS terciário que será consultado se o primário e o secundário estiverem fora do ar. Ele é opcional.

Aba de Dispositivos de Rede

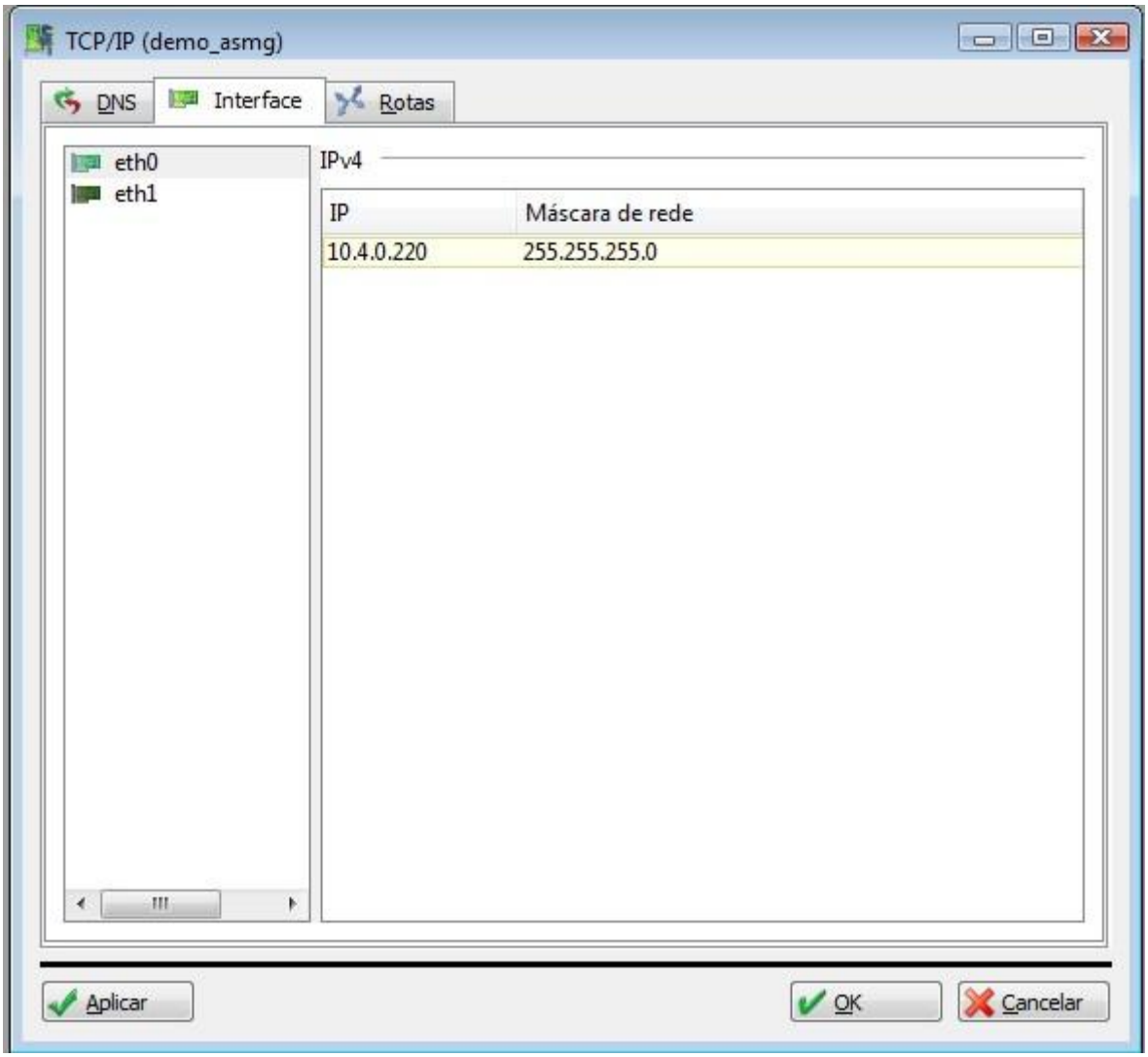

Figura 48. TCP/IP – Interface.

Nesta pasta podem ser configurados os endereços IP atribuídos a todas as interfaces de rede reconhecidas pelo ASMG. Ela consiste de uma lista onde são mostrados os nomes de todas as interfaces e os endereços IP e máscaras de cada uma (é possível configurar até 31 endereços distintos para cada interface). Caso uma interface não tenha um endereço IP configurado, os campos correspondentes ao endereço e à máscara serão mostrados em branco. Possui os seguintes campos:

© Aker Security Solutions

Dispositivos: Considera-se também a interface na criação da rota.

IP: Endereço da rede. Não pode ser informado um endereço auto-configurado.

Máscara de rede: Máscara de rede.

Para configurar ou modificar o endereço IP ou máscara de uma interface e até mesmo atribuir um *alias* para a interface, deve-se clicar sobre a entrada do dispositivo correspondente e usar o menu suspenso que irá surgir:

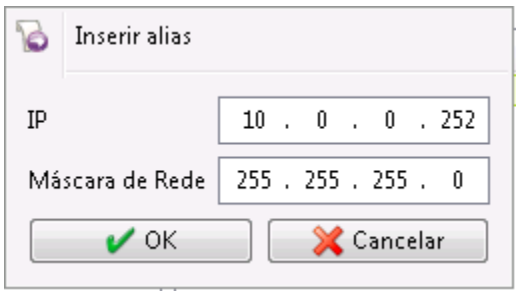

Figura 49. Menu suspenso – inserir alias.

Só é possível configurar endereços IP de interfaces de rede reconhecidas pelo sistema operacional no qual o ASMG está rodando. Caso tenha acrescentado uma nova interface de rede e seu nome não apareça na lista de interfaces, é necessário configurar o sistema operacional de forma a reconhecer esta nova interface antes de tentar configurá-la nesta pasta.

O IP e o prefixo têm que ser informados juntos.

Não deverá ser possível ao usuário remover ou editar os endereços autoconfigurados (são derivado dos endereços MAC).

As interfaces que estiverem em vermelho, indicam que não estão presentes em todos os nodos do cluster.

Nesta pasta podem ser configurados os endereços IP atribuídos a todas as interfaces de rede reconhecidas pelo sistema operacional. Ela consiste de uma lista onde são mostrados os nomes de todas as interfaces e os endereços IP e máscaras de cada uma (é possível configurar até 31 endereços distintos para cada interface). Caso uma interface não tenha um endereço IP configurado, os campos correspondentes ao endereço e à máscara serão mostrados em branco.

© Aker Security Solutions

Aba de Rotas

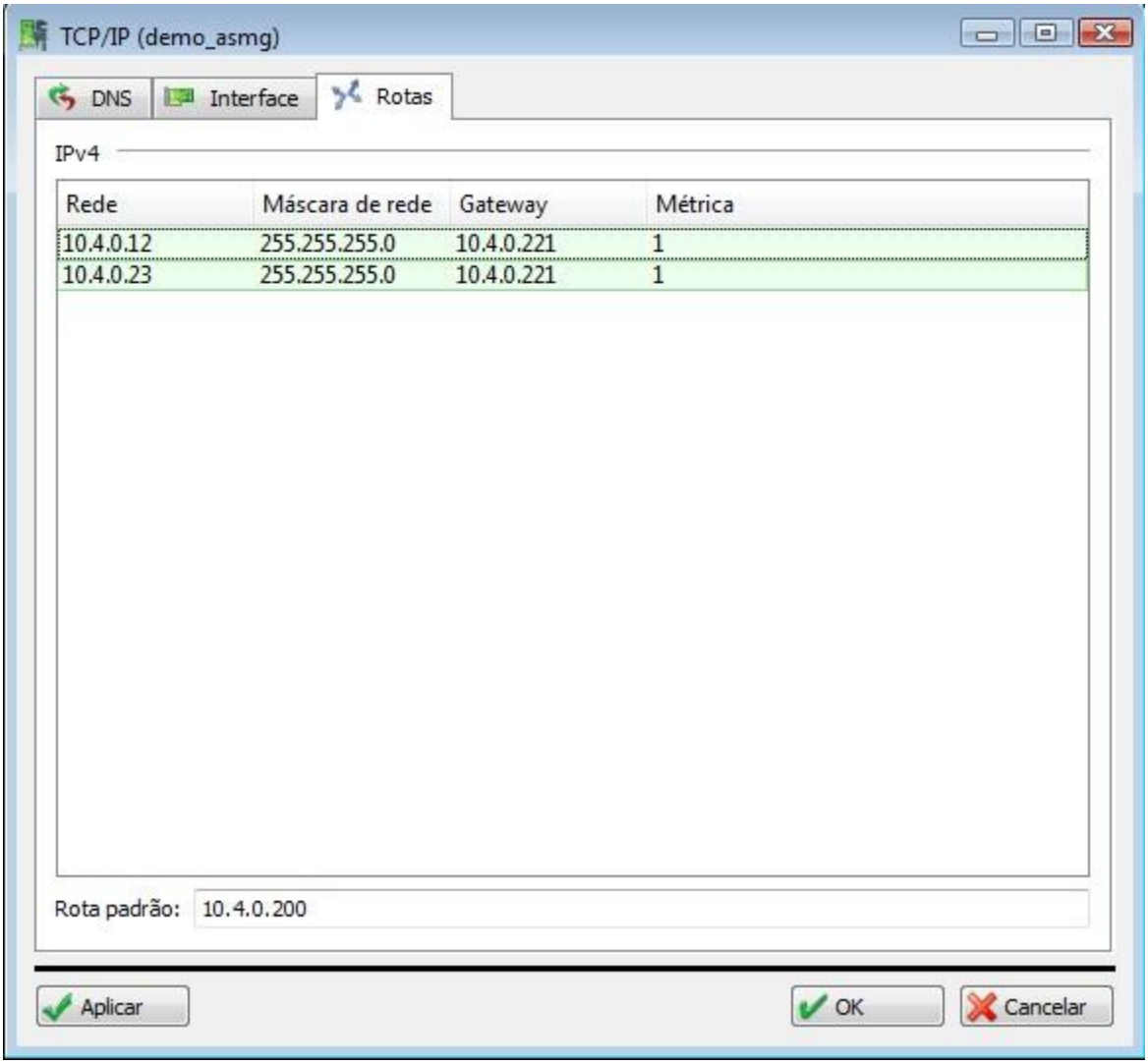

Figura 50. TCP/IP - Rotas.

Esta pasta possibilita configurar rotas IP no ASMG. Ela consiste de um campo, chamado de "**Rota Padrão"**, onde pode especificar o roteador padrão e de uma lista com as diversas rotas configuradas no ASMG.

Para a inclusão de uma nova rota, basta clicar no botão direito do mouse e irá aparecer o menu "Inserir Rotas".

Para remover ou editar uma rota, basta clicar com o botão direito sobre ela.

Rede: Configuração dos endereços IP

Máscara de rede: Máscara de rede

Gateway: Nesse campo deve ser informado o endereço IP do roteador.

Métrica: Este campo define o peso associado à rota, este peso é utilizado na definição da melhor rota, quando se utiliza roteamento dinâmico. No caso de roteamento estático, o campo é ignorado.

© Aker Security Solutions

Confirmação de E-mail

7. Confirmação de E-mail

A confirmação de mensagens é um recurso oferecido pelo **ASMG** bastante eficiente no combate a SPAMs. Spammers geralmente utilizam endereços inválidos quando enviam mensagens, com a intenção de "burlar" a vigilância.

O sistema funciona da seguinte maneira: ao enviar uma mensagem pela primeira vez para um domínio intermediado pelo **ASMG,** o remetente tem sua mensagem retida por um período de tempo e recebe uma mensagem de notificação do sistema. Esta mensagem possui um link que deve ser visitado pelo remetente, a fim de "confirmar" sua existência.

Ao executar esta tarefa, o remetente tem seu endereço adicionado à lista automática de endereços autorizados, a *whitelist,* e sua(s) mensagem(s) são entregue ao(s) destinatário(s). A partir deste momento, o remetente não precisa mais realizar este procedimento para novas mensagens enviadas aos domínios intermediados pelo **ASMG**, mesmo que sejam destinadas a outros usuários.

O sistema de confirmação possui grande flexibilidade de configuração. Se o Administrador assim desejar, cada usuário do domínio poder decidir sobre a utilização ou não do sistema em mensagens enviadas para ele, além de poder escolher os parâmetros de configuração também particulares para ele. A administração destas opções é feita através da Interface do Usuário, que será explicada na "**Interface Gráfica do Usuário".**

O sistema de confirmação de mensagens possui diversas janelas de configuração que devem ser configuradas adequadamente. Para tanto, será mostrado cada um e explicado como deve ser feito.

Aliases

O termo **"Alias"** é usado para designar, no contexto de mensagens eletrônicas, um usuário especial do domínio. Não representa um usuário real, mas sim um apelido dado a um ou mais usuários válidos. Normalmente são criados com o nome de funções ou áreas especiais dentro de uma empresa, constituindo importante mecanismo de comunicação com clientes, parceiros, fornecedores e colaboradores, e imprimindo um caráter não pessoal e institucional ao mecanismo de comunicação por mensagens eletrônicas. Como exemplos de nomes comuns para estes apelidos, podemos citar "diretor", "ouvidoria", "gerencia", "logística", entre outros. Um alias é, ao final, "traduzido" pelo servidor de e-mail em um conjunto de um ou mais nomes de usuários reais. Ao final, estes usuários são os que receberão de fato os e-mails enviados aos aliases.

© Aker Security Solutions

No contexto do ASMG, o uso de aliases pode representar um problema para o sistema de confirmação de mensagens. Afinal, este sistema possui a opção de configuração individual, por usuário (para maiores detalhes, veja a subseção a seguir). Como os nomes de aliases só são traduzidos em nomes de usuários reais após a passagem da mensagem pelo ASMG, a princípio o produto não tem como saber a qual usuário real um determinado alias se refere. Por exemplo, suponha um usuário "joao@seudominio.com", que recebe os e-mails enviados para o alias "vendas@seudominio.com". Neste contexto, as configurações para o sistema de confirmação do usuário só serão consideradas caso o e-mail seja enviado para o destinatário real. Caso sejam enviados para "vendas@seudominio.com", tal configuração não será considerada e os e-mails não serão filtrados conforme o esperado.

Para contornar este problema, o ASMG oferece a opção de cadastro de aliases. A partir desse cadastro, um usuário da rede consegue acessar a interface do usuário utilizando o alias ao invés do próprio nome, configurando assim as opções para o sistema de confirmação específico para e-mails enviados ao alias. O ASMG disponibiliza dois tipos de registros de alias, conforme explicaremos a seguir.

Apenas a criação do aliases não garante o uso do sistema de confirmação para e-mails enviados a ele. Além disso, é necessário logar pelo menos uma vez na interface do usuário, oferecendo como login o nome do alias criado, assim como deve ser feito por usuários reais na configuração onde se escolhe aplicar a confirmação apenas para usuários cadastrados.

Alias Associado à Senha

Este tipo de alias pode ser encarado como um alias completo, pois requisita a designação de um nome para o alias e também o de uma senha associada, a fim de que ambos sejam utilizados no acesso à interface do usuário.

Para criar este tipo de alias, é necessário escolher a opção "Associar Alias a senha" e preencher as informações requisitadas nos campos **"Nome"**, **"Descrição"**, **"Senha"** e **"Confirmação"** com os dados referentes ao alias. Em seguida, basta clicar no botão **"Aplicar"**.

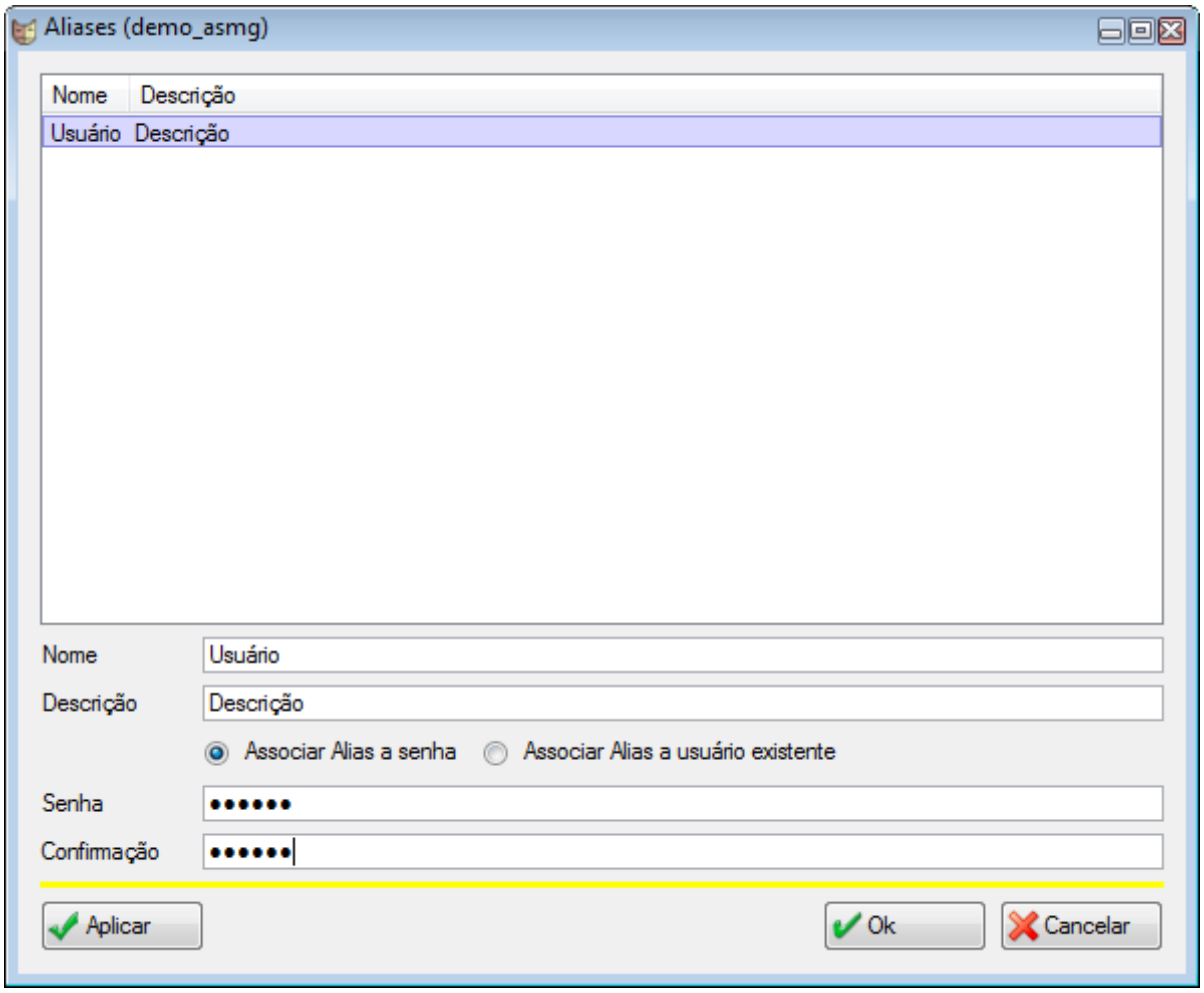

Figura 51. Aliases associados a senhas.

O nome oferecido para o alias **não deve incluir o domínio.** Contudo, ao utilizar o alias para acesso à interface do usuário, este **deve necessariamente digitar o nome do alias seguido de @ e de seu domínio válido, conforme faz para seu usuário real.** A idéia é que um mesmo alias possa ser aproveitado para utilização com diferentes domínios, ou seja, que não haja a necessidade de criação de diferentes aliases para diferentes domínios.

Alias Associado a usuário existente

Neste tipo de alias é criado apenas um nome, e este nome é então associado a um usuário válido da rede, de modo que a senha deste último possa ser aproveitada para a autenticação do alias na interface do usuário.

Para criar este tipo de alias, é necessário escolher a opção **"Associar Alias a usuário existente"** e preencher as informações requisitadas nos campos **"Nome"**, **"Descrição"** e **"E-mail do Usuário"** com os dados desejados. Note que o parâmetro que relaciona o alias a um usuário é o e-mail completo do usuário real. Em seguida, basta clicar no botão **"Aplicar"**.

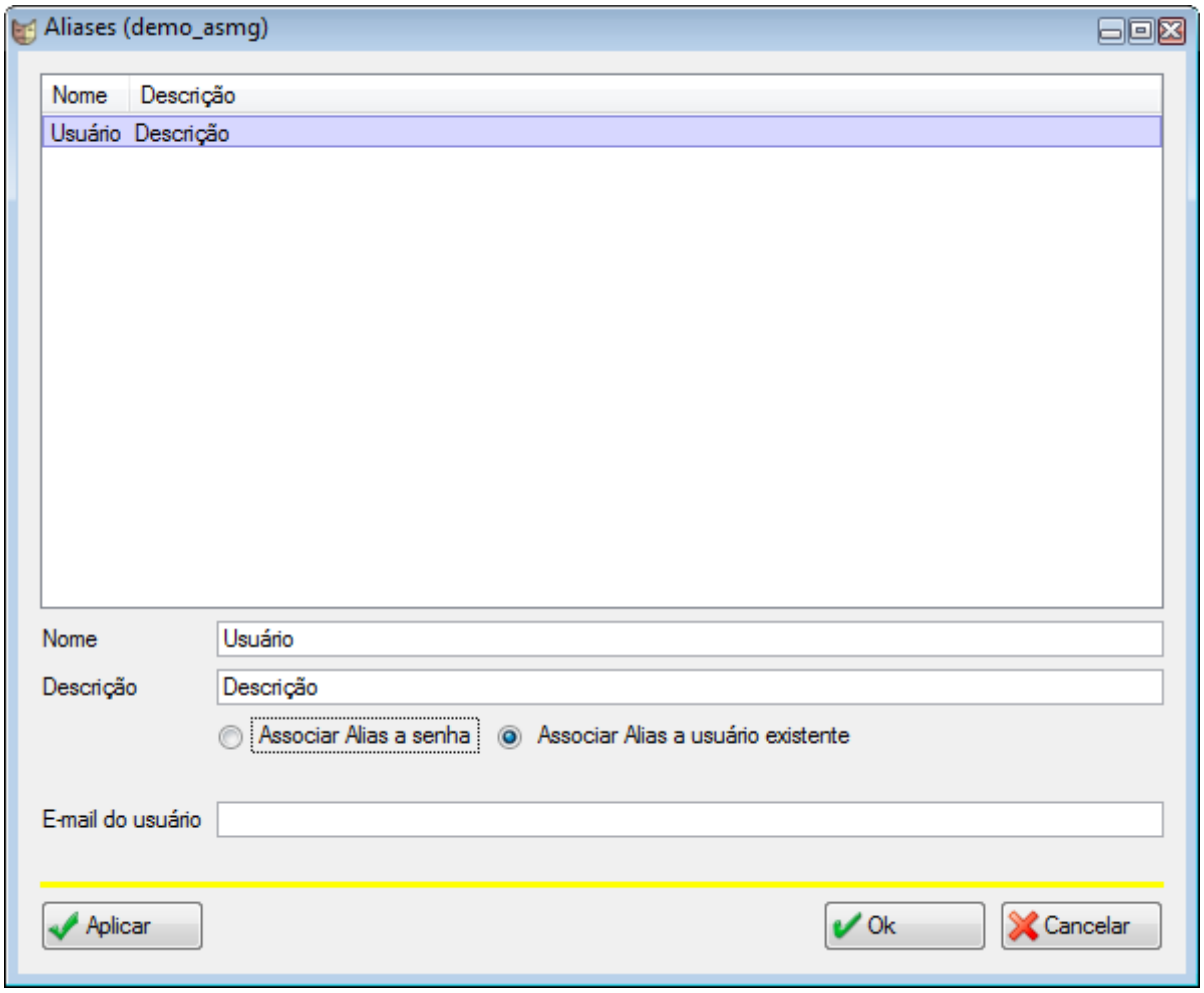

Figura 52. Aliases associados a usuário existente.

Como no caso anterior, o nome oferecido para o alias não deve incluir o domínio. Contudo, ao utilizar o alias para acesso à interface do usuário, este deve necessariamente digitar o nome do alias seguido de @ e de seu domínio válido, conforme faz para seu usuário real.

É possível criar e modificar aliases a partir de um binário de linha de comando no ASMG. Para tanto, basta utilizar o comando /aker/bin/asmg/loginif**.** Ao invocar o comando sem nenhum parâmetro, será apresentada uma lista completa de opções e sintaxe de uso.

Associação de domínios

Esta janela possibilita o uso de um autenticador comum para diferentes domínios que usam a confirmação de e-mail. Nela é possível definir qual é o domínio principal, seu autenticador, e quais domínios usarão o autenticador desse domínio.

Um uso comum dessa janela é fazer com que os subdomínios utilizem o

© Aker Security Solutions

autenticador do domínio raiz para fazer a autenticação de usuários na webgui de confirmação do usuário. Exemplo: e-mails do domínio sp.aker.com.br usariam o autenticador do domínio raiz aker.com.br

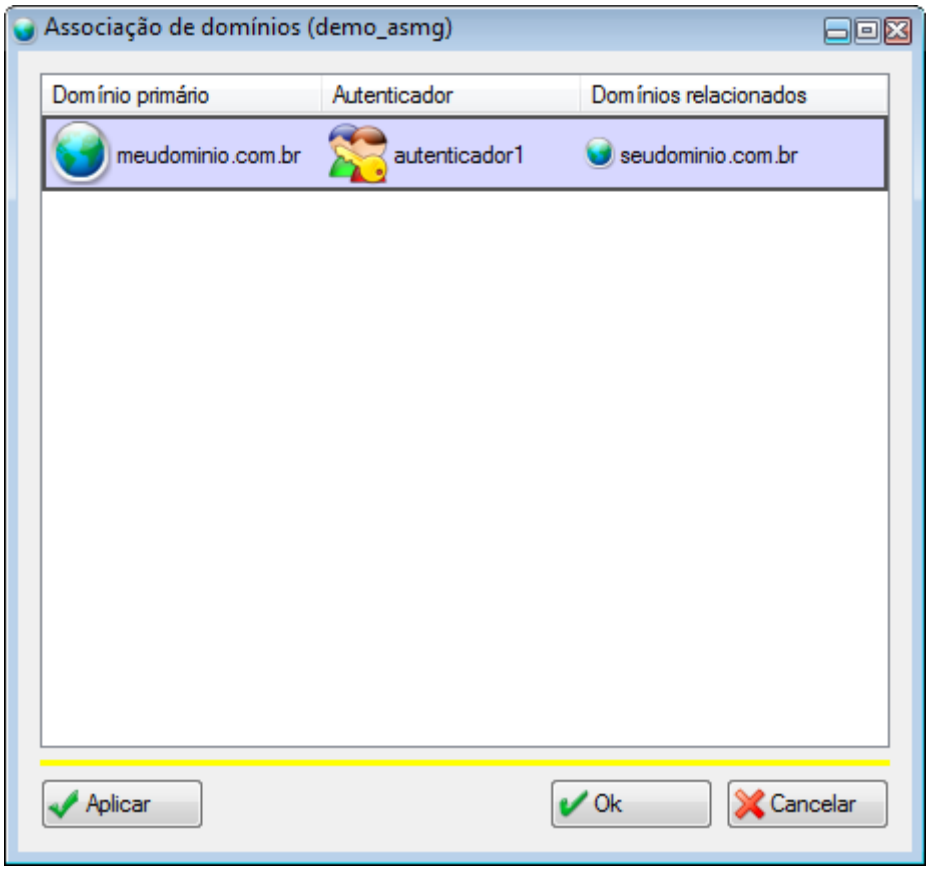

Figura 53. Associação de domínio.

Esta opção irá resolver o problema das empresas que possuem dois ou mais domínios associados à mesma caixa postal, exemplo:

Uma Empresa possui os domínios "meudominio.com.br" e o "nossodominio.com.br", caso sejam encaminhadas mensagens para "joao@meudominio.com.br" ou para "joao@nossodominios.com.br", ambos serão recebidos pelo mesmo destinatário, com isso há necessidade de se associar todos os domínios da empresa entre eles. Assim o sistema de **"Confirmação de E-mail"** funcionará de forma transparente para todos os domínios, mantendo apenas uma Interface do Usuário, com configurações unificadas.

Configuração Geral

Esta janela apresenta todos os parâmetros de configuração geral da funcionalidade de confirmação de mensagem.

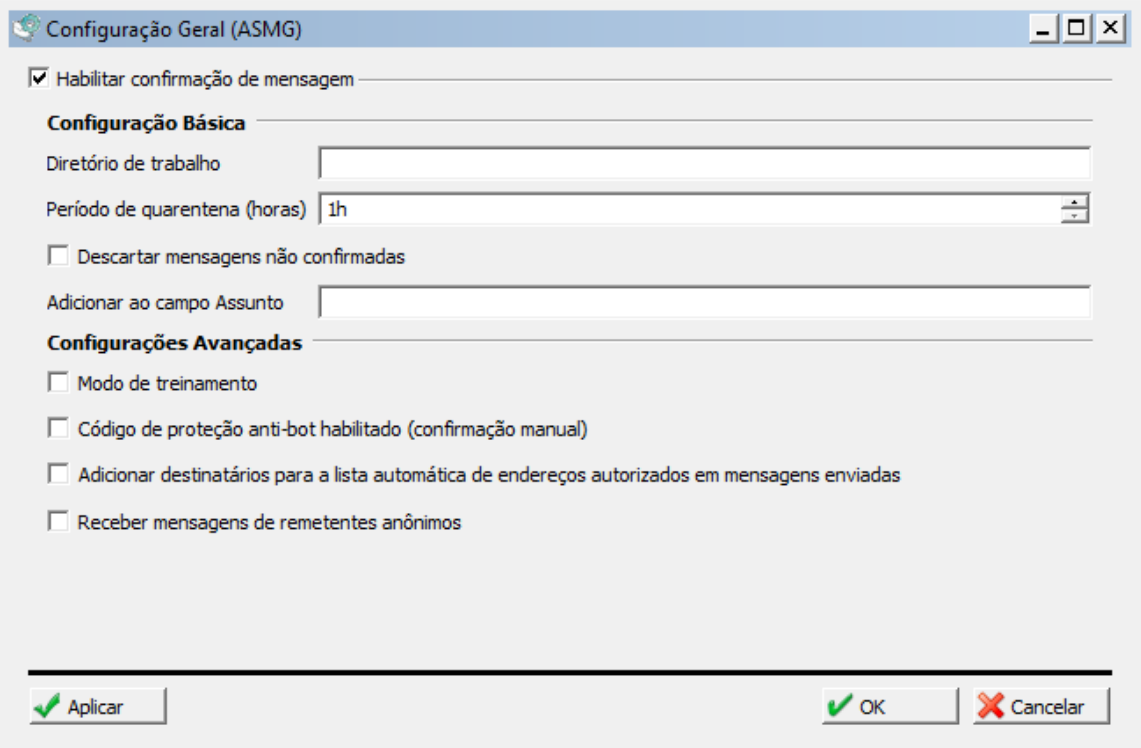

Figura 54. Configuração geral do ASMG.

Configuração Básica

Nesta parte pode-se definir o diretório de trabalho, ou seja, o local onde os arquivos de configuração relativos ao sistema de confirmação, inclusive os arquivos de configuração particulares de cada usuário da rede, devem ser armazenados. Pode-se também definir o tempo de espera, em horas, através da opção **"Período de quarentena"**.

Para o caso de mensagens não confirmadas ao fim do período de quarentena definido pelo parâmetro anterior, existem duas possíveis opções de configuração: a primeira delas é a exclusão de mensagens não confirmadas. Para escolher este comportamento, basta marcar a opção **"Descartar mensagens não confirmadas"**. Caso este campo não esteja marcado, tem-se a segunda opção de configuração, onde a mensagem é entregue ao(s) destinatário(s) sendo necessário inserir uma mensagem no campo **"Assunto"** da mensagem para que este(s) saiba facilmente que se trata de uma mensagem não confirmada. Para escolher esta opção, basta inserir a mensagem desejada em **"Adicionar ao campo assunto"**.

Configurações Avançadas

Esta parte apresenta algumas opções importantes. São elas:

Modo de treinamento

Com esta opção ativada, o sistema de confirmação de mensagem armazena todos os endereços de e-mails dos remetentes na Whitelist dos destinatários protegidos pelo ASMG, sem que nenhum e-mail seja bloqueado pela confirmação.

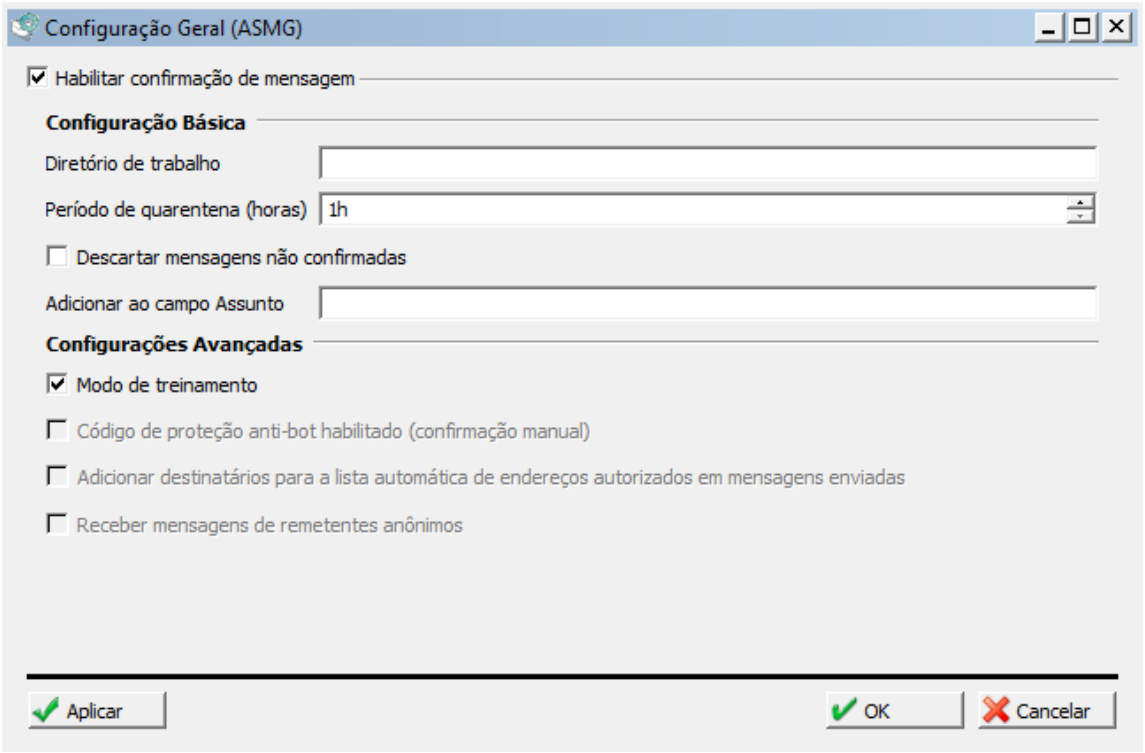

Figura 55. Configuração Modo de treinamento.

A configuração do **"Modo de Treinamento"** na janela de **"Configuração Geral"** faz com que todos os usuários entrem em **"Modo de Treinamento"**, indepedendente da configuração individual do usuário.

Inicialmente, a configuração de todos os usuários está no **"Modo de Treinamento"**. A confirmação somente passa a ser solicitada após o usuário configurar a Interface de **"Usuários".**

Todos os usuários podem, a qualquer momento, desabilitar seu uso do sistema de confirmação, a partir da "Interface gráfica do usuário".

Código de proteção anti-bot habilitado (confirmação manual):

Se esta opção estiver habilitada, a operação de confirmação, que deve ser efetuada pelo remetente da mensagem após receber a mensagem de confirmação, só será efetuada mediante digitação de código de proteção. Tal opção impede que robôs façam a confirmação automática da mensagem e seu uso é recomendado. Caso contrário, a confirmação limita-se à visitação da URL contida na mensagem de confirmação que é enviada ao remetente da mensagem.

Adicionar destinatários para a lista automática de endereços autorizados em mensagens enviadas:

Esta opção, quando habilitada, automaticamente adiciona à lista de endereços autorizados os destinatários de mensagens enviadas pelos usuários da rede. Se levarmos em conta que os usuários internos enviam mensagens para pessoas conhecidas, isto retira a necessidade de confirmação por parte deste usuário num e-mail de resposta, por exemplo.

Receber mensagens de remetentes anônimos:

Remetentes anônimos são utilizados por servidores de e-mail para envio de mensagens de sistema, e isto é permitido pela recomendação do SMTP. Contudo, este recurso pode também ser utilizado por spammers para que a mensagem consiga ultrapassar o sistema de confirmação.

Se você optar por não receber mensagens do sistema, esteja ciente de que poderá deixar de receber mensagens de sistema autênticas.

Lista Automática

Nesta janela pode-se visualizar endereços contidos na lista automática de endereços autorizados, ou seja, na lista de remetentes que já efetuaram confirmação. O Administrador pode se desejar, remover elementos dessa lista.

Para fazer uma pesquisa de endereços, basta digitar o nome no campo **"Localizar Padrão"** e, em seguida, clicar no botão **"Carregar"**, localizado na barra de tarefas do Aker Control Center.

Também é possível remover endereços que estejam nesta listagem. Para isso, basta selecionar o(s) endereço(s) que desejar remover e selecionar a opção **"Remover"**, presente na barra de tarefas.

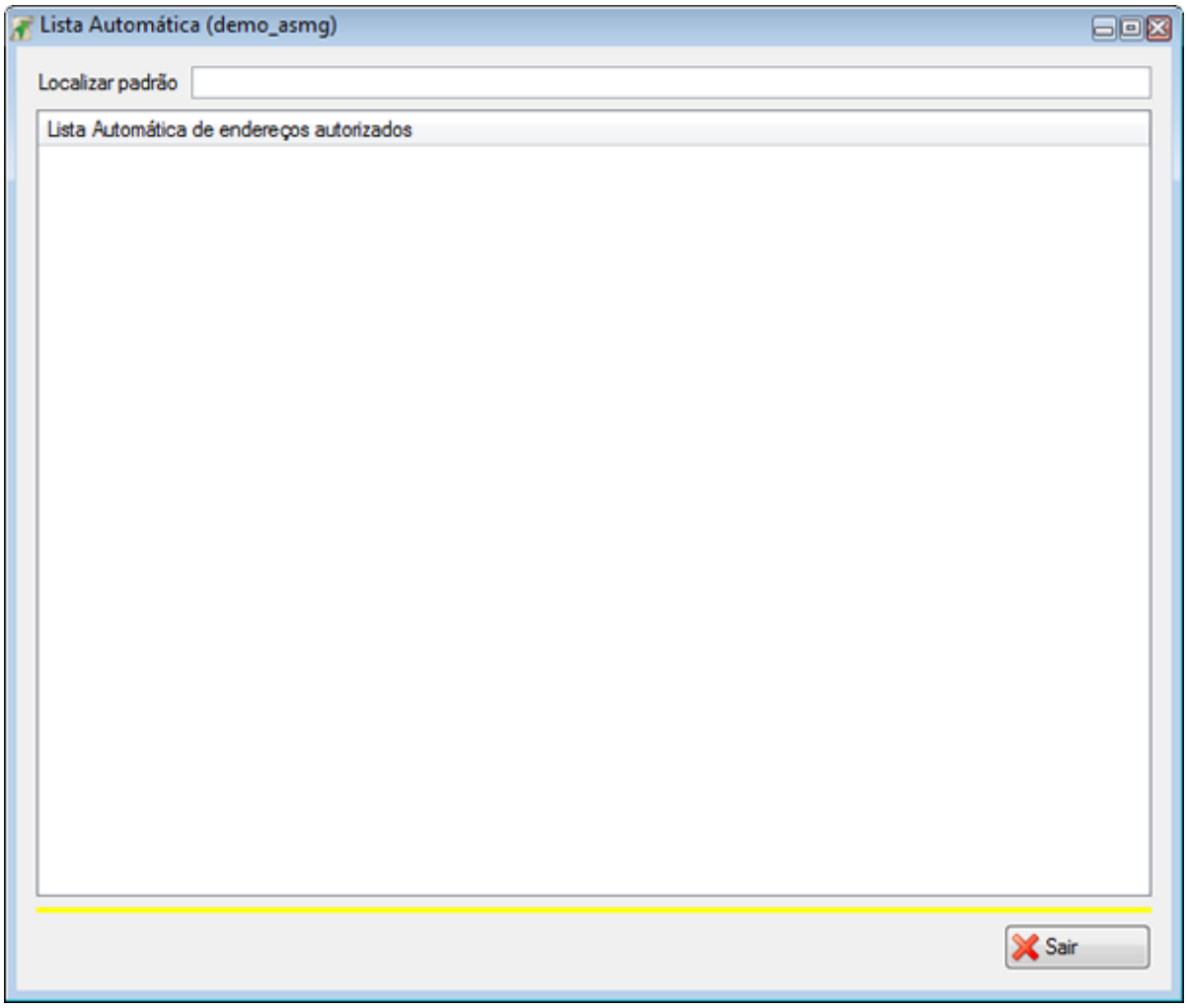

Figura 56. Lista automática.

Não é obrigatório digitar algum conteúdo no campo **"Localizar Padrão"** para efeito de apresentação dos endereços que compõem a lista atual. Este campo deve ser utilizado para questões de filtragem.

A remoção de um nome da lista automática não impede que o remetente retorne a essa mesma lista. Caso ele envie nova mensagem para destinatário do domínio e a confirme, voltará para a lista automática. Para a exclusão definitiva de um endereço é necessário fazer esta remoção e também a inclusão do endereço na lista manual de endereços não autorizados, conforme explica a subseção a seguir.

Listas Manuais

Nesta janela configuram-se as listas globais de endereços autorizados, endereços proibidos e assuntos autorizados. As listas são ditas globais porque valem para todos os usuários que possuírem confirmação ativa.

O campo **"Lista manual de endereços autorizados"** reúne endereços de remetentes que não devem receber pedidos de confirmação e nem possuem a mensagem retida para confirmação (*whitelist*).

O campo **"Lista manual de endereços não autorizados"** reúne remetentes que não podem enviar mensagens para os domínios intermediados pelo **ASMG**.

Finalmente, o campo **"Lista manual de assuntos autorizados"** normalmente é utilizado para evitar que mensagens enviadas com destino a grupos de discussão, dos quais usuários de uma rede intermediada pelo **ASMG** façam parte, sejam retidas para confirmação. Neste caso, a partir da análise do assunto da mensagem, o sistema pode permitir que ela alcance seu destino de maneira imediata. Para tanto, basta especificar nesta listagem quais são os assuntos, de forma idêntica ou como substring, que caracterizam mensagens as quais não devem ser retidas para confirmação, independente de quem seja o remetente ou destinatário.

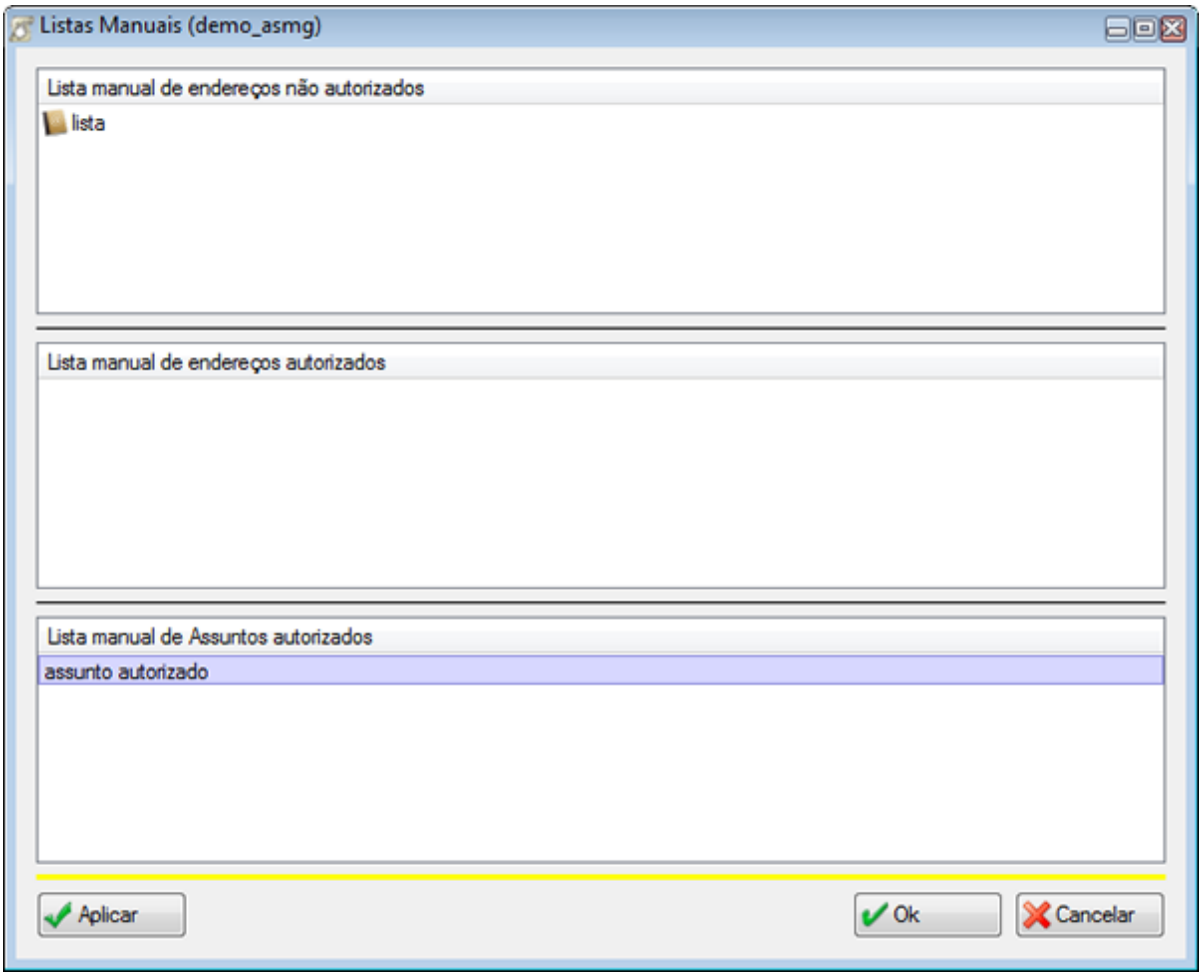

Figura 57. Lista manual.

As listas a que se refere esta janela são de uso exclusivo do sistema de confirmação e não são aproveitadas pelos outros filtros do sistema.

Mensagem Modelo

Nesta janela devem-se inserir os dados referentes à mensagem de confirmação que será enviada a um remetente ainda desconhecido pelo sistema de confirmação. Dentre as informações importantes é necessário indicar a URL da página de confirmação, o assunto da mensagem e se o assunto da mensagem original deve ser referenciado ou não.

A mensagem propriamente dita deve ser escrita no quadro **"Conteúdo da mensagem de confirmação"**. A fim de que o texto da mensagem seja convertido à linguagem HTML, é necessário clicar sobre o botão **"Gerar mensagem modelo"**. Mesmo com a geração automática da mensagem, ainda é possível que o Administrador personalize seu conteúdo.

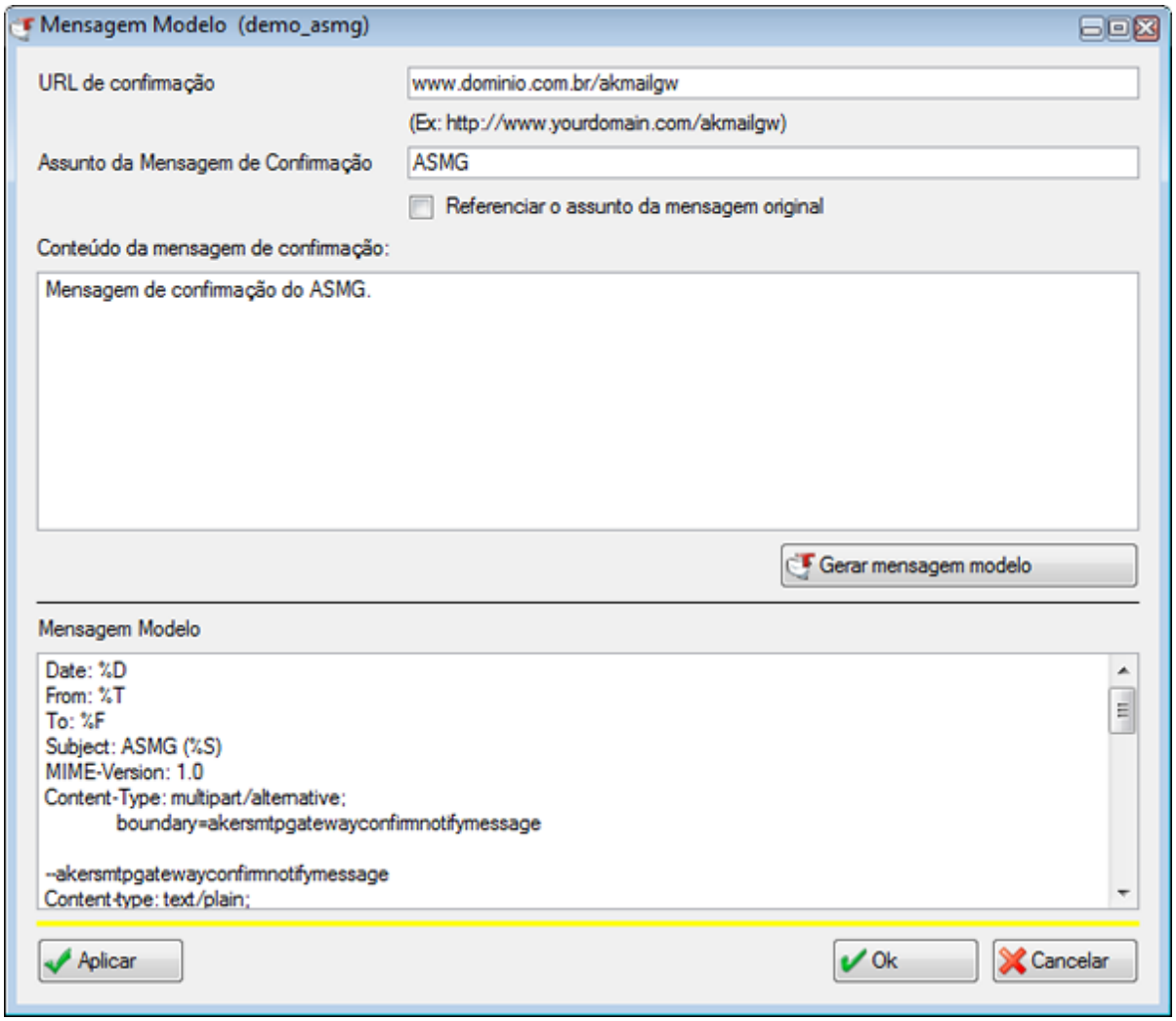

Figura 58. Mensagem modelo.

Visualizador de Quarentena

Esta tela mostra o acesso a todas as mensagens que estão em quarentena, aguardando confirmação.

Para fazer uma pesquisa, basta digitar o endereço do destinatário que deseja consultar no campo **"E-mail do Usuário"** e clicar no botão **"Carregar"**, localizado na barra de ferramentas do Aker Control Center. Quando a mensagem for localizada, pode-se cancelar sua entrega ou, conforme o caso, decidir por entregá-la imediatamente.

Se a mensagem for retirada da quarentena manualmente, o usuário não será adicionado à *whitelist*. Esta ação apenas retira a mensagem da quarentena e a encaminha para o usuário correspondente.

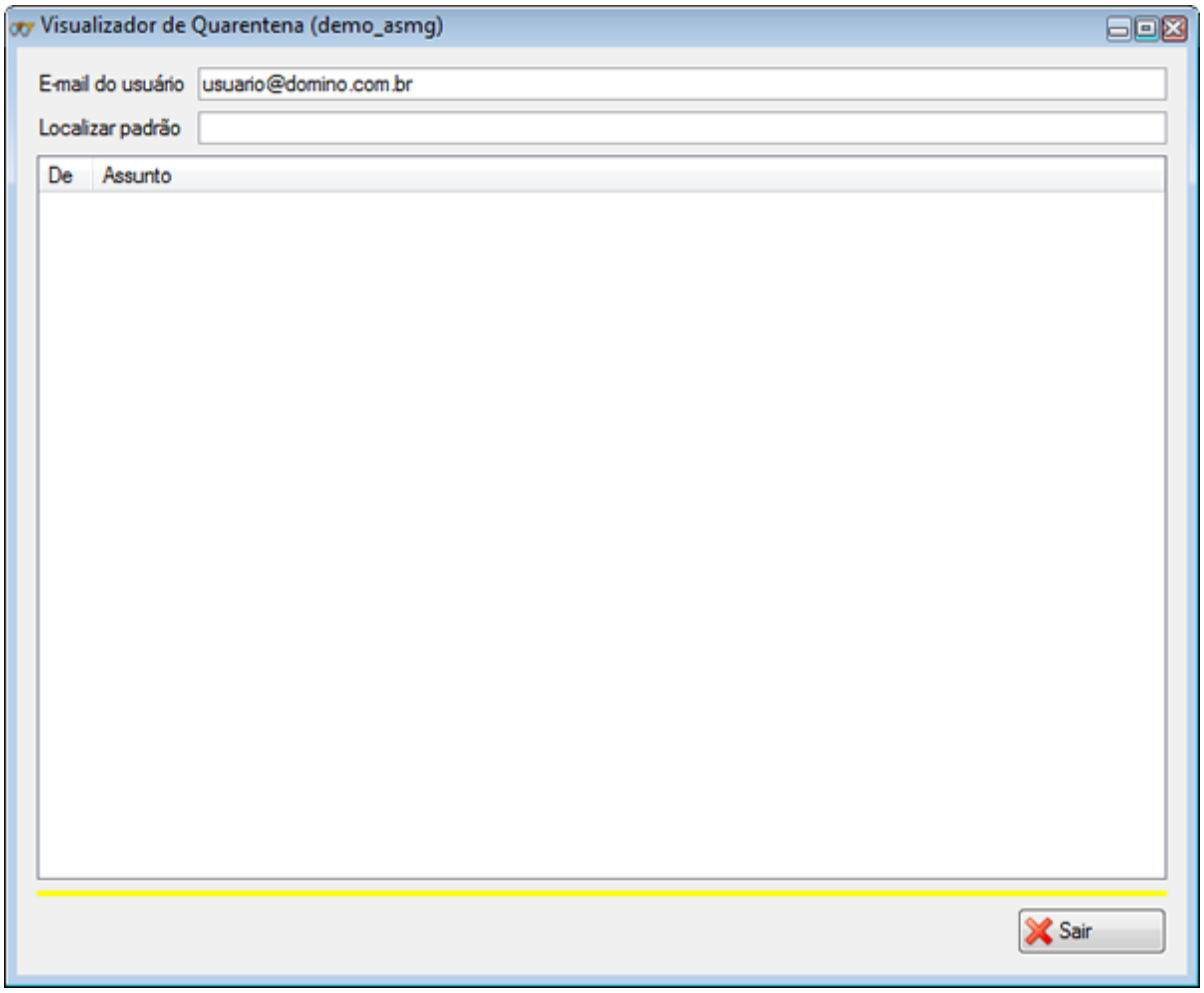

Figura 59. Visualizador de quarentena.

Filtragem de Conexão

8. Filtragem de conexão

O item **"Filtragem de conexão"** compreende uma série de regras que serão aplicadas igualmente a todos os usuários de redes intermediadas pelo **ASMG**.

Desta maneira, as configurações feitas através deste item serão estendidas para todas as políticas e grupos que forem criados dentro do **ASMG**.

Esse item compreende as seguintes opções:

- Controle de Flood;
- RBLs;
- Sender-ID/SPF;
- Servidores, Domínios e Redes.

Controle de Flood

Flood é um termo utilizado para indicar uma "inundação" de conexões ou mensagens em curto espaço de tempo. Isso quer dizer que ocorre um número enorme de requisições simultâneas de serviço que podem causar interrupção no serviço de correio. Normalmente o Flood faz parte de algum ataque de usuários maliciosos com fins escusos.

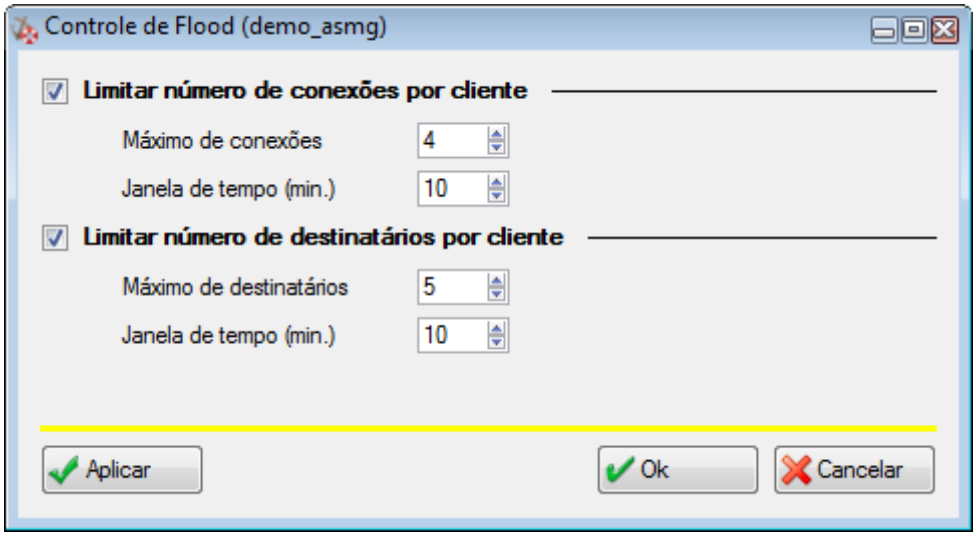

Figura 60. Controle de Flood.

Esta janela está dividida em duas partes:

Limitar número de conexões por cliente

Quando esta regra está habilitada, podemos definir o limite de conexões simultâneas que um cliente pode estabelecer em determinado espaço de tempo, medido em minutos.

Limitar número de destinatários por cliente

Aqui pode-se definir para quantos destinatários em uma mesma mensagem um cliente externo pode enviar mensagens, e a janela de tempo, em minutos, que ele deve esperar entre um envio e outro.

RBLs

Nesta janela deve-se referenciar as listas do tipo RBL, já previamente cadastradas, que devem ser utilizadas como apoio à consulta atualizada de servidores promíscuos, comumente utilizados por spammers.

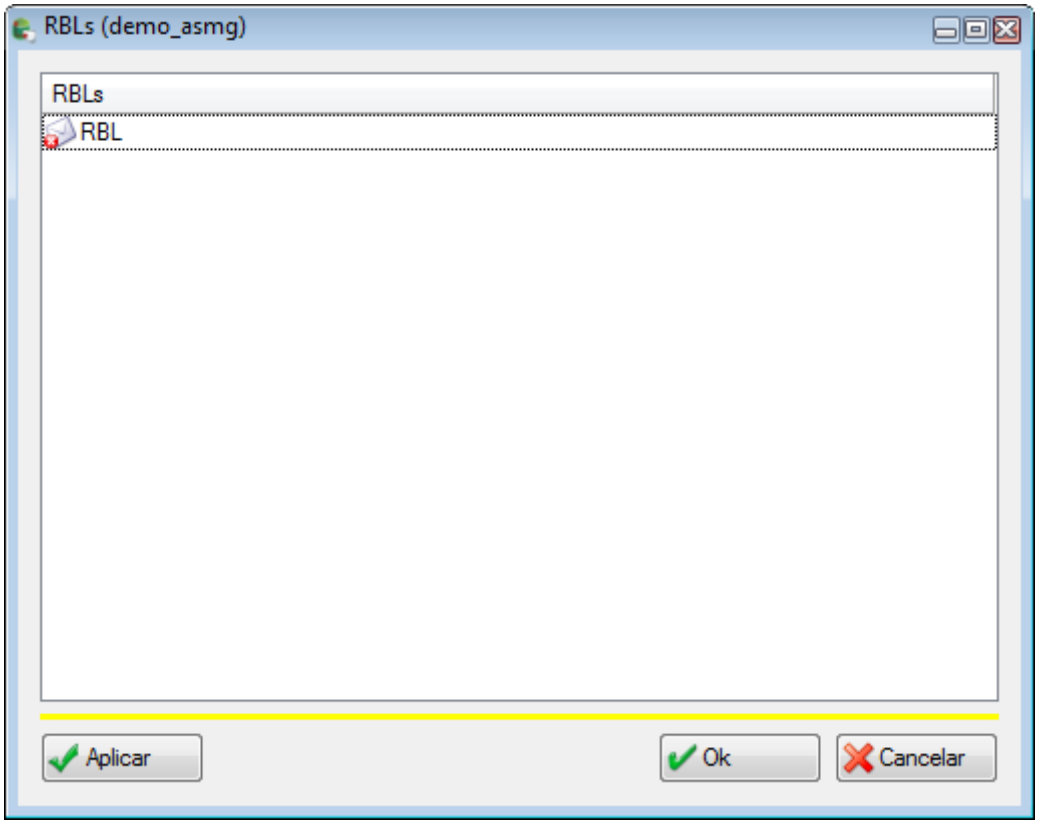

Figura 61. Referenciar as listas do tipo RBL.

Para incluir uma entidade do tipo "RBL", clique com o botão direito do mouse sobre o quadro e escolha a opção **"Adicionar Entidades"**. A seguir, escolha a(s) entidade(s) desejada(s) e clique em **"Adicionar"**.

Sender-ID/SPF

Como o protocolo SMTP não possui autenticação própria, os spammers se utilizam desta vulnerabilidade para enviar e-mails em nome de outras pessoas. Um caso muito comum hoje em dia é quando um determinado usuário **X** recebe uma mensagem vinda de um remetente **Y** quando, na verdade, **Y** não enviou nenhuma mensagem. Esta vulnerabilidade torna necessário um mecanismo de autenticação externa a fim de assegurar se a fonte da mensagem é real ou não. Os dois padrões utilizados atualmente são o *SPF* e o *Sender-ID*.

O padrão SPF permite que, através de uma configuração simples no DNS de determinado domínio, seja adicionada uma linha de texto com a informação que descreve quais os endereços dos servidores de e-mail que estão autorizados a gerar mensagens daquele domínio (MX-reverso).

Já o Sender-ID é a junção do padrão SPF com o PRA, e tem como objetivo validar o protocolo usado no endereço de quem enviou uma mensagem, detectando seu remetente e facilitando a filtragem do lixo eletrônico.

Para habilitar a filtragem, basta marcar a caixa **"Habilitar filtragem de Sender-ID/SPF"**. É possível ainda recusar ou aceitar mensagens de clientes não autorizados e, opcionalmente, movê-las para a quarentena ou encaminhá-las para um grupo de e-mail específico.

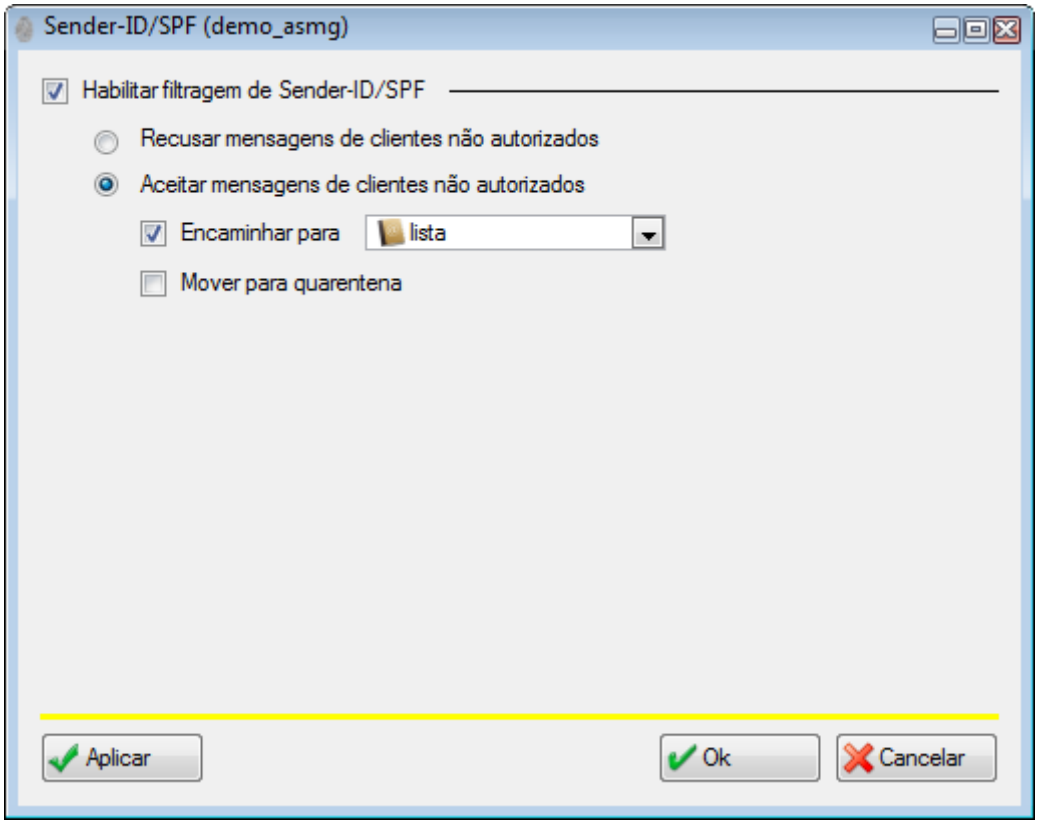

Figura 62. Sender ID/SPF.

Servidores, Domínios e Redes

Esta janela trata de filtragens diretamente ligadas a filtros de conexão, especificados os servidores, por endereço individual, nome ou rede, que estão autorizados a negociarem mensagens com o ASMG e aqueles que não estão autorizados a fazerem este procedimento. Esta janela é composta de pelas abas **"Lista de Endereços Autorizados"** e **"Lista de Endereços não Autorizados".**

Temos a opção **"Rejeitar clientes sem DNS reverso",** uma vez marcada o ASMG fará a checagem para determinar a existência do DNS reverso, caso não exista irá bloquear a conexão destes clientes.

A seguir será abordado detalhadamente as funcionalidades de cada aba:

Aba Lista de endereços autorizados

É composta pelos quadros Servidores, Domínios e Redes. Nela informamos as Entidades (já previamente cadastradas) que devem ter suas conexões aceitas por todos os filtros de conexão sem que haja sequer execução da filtragem. Em resumo, esta aba armazena uma whitelist de servidores. As filtragens que são atingidas por esta configuração são:

- RBL
- Gray Listing
- Controle de Flood
- Sender-ID/SPF

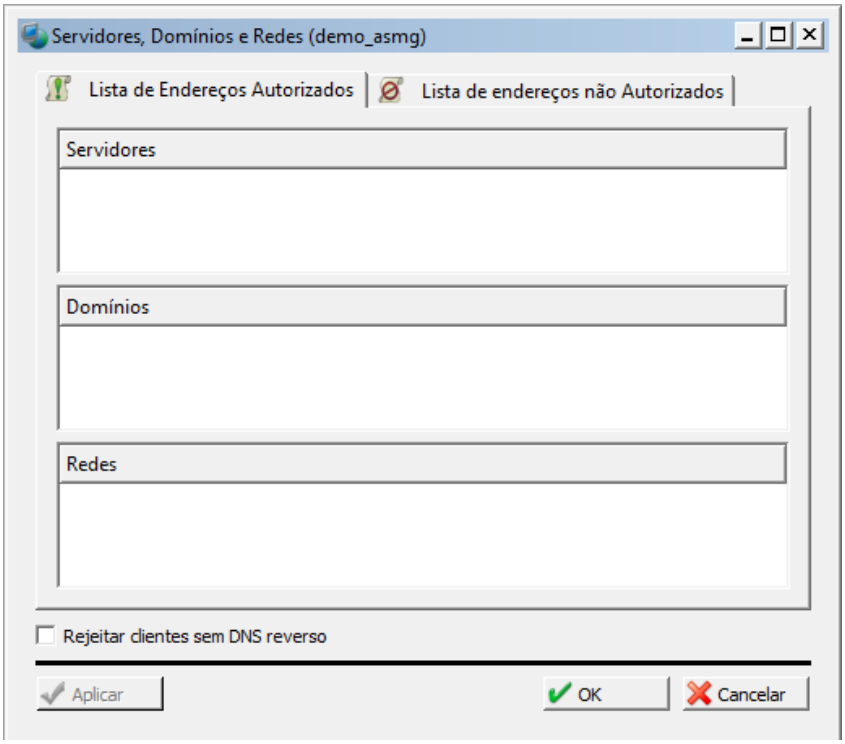

Figura 63. Lista de endereços autorizados.

Utilize esta opção com o devido cuidado, pois na prática ela vai desabilitar os filtros mencionados acima sempre que o servidor com o IP configurado em uma das ações da janela estabelecer uma conexão com o ASMG.

Servidores

Para referenciar uma entidade do tipo "Servidor" com conexão permitida, clique com o botão direito do mouse sobre ele e escolha a opção **"Adicionar Entidades"**. A seguir, escolha a entidade cuja conexão deva ser permitida e, em seguida, clique em **"Adicionar"**.

Domínios

Para referenciar uma entidade do tipo **"Domínio"** que tenha conexão permitida, clique com o botão direito do mouse sobre ele e escolha a opção **"Adicionar Entidades"**. A seguir, escolha a entidade cuja conexão deva ser permitida e clique em **"Adicionar"**.

Esta opção incluirá na whitelist de conexões todos os servidores que tiverem parte do domínio escolhido por resolução de DNS Reverso.

Redes

Para referenciar uma entidade do tipo **"Redes"** com conexão permitida, clique com o botão direito do mouse sobre o quadro **"Redes"** e escolha a opção **"Adicionar Entidades"**. A seguir, escolha a entidade cuja conexão deva ser permitida e clique em **"Adicionar"**.

Aba Lista de endereços não-autorizados

Esta aba também é composta pelos quadros Servidores, Domínios e Redes, mas a diferença é que nela deve-se informar as Entidades (já previamente cadastradas) que devem ter suas conexões sempre recusadas. Armazena, portanto, uma blacklist de conexões.

© Aker Security Solutions

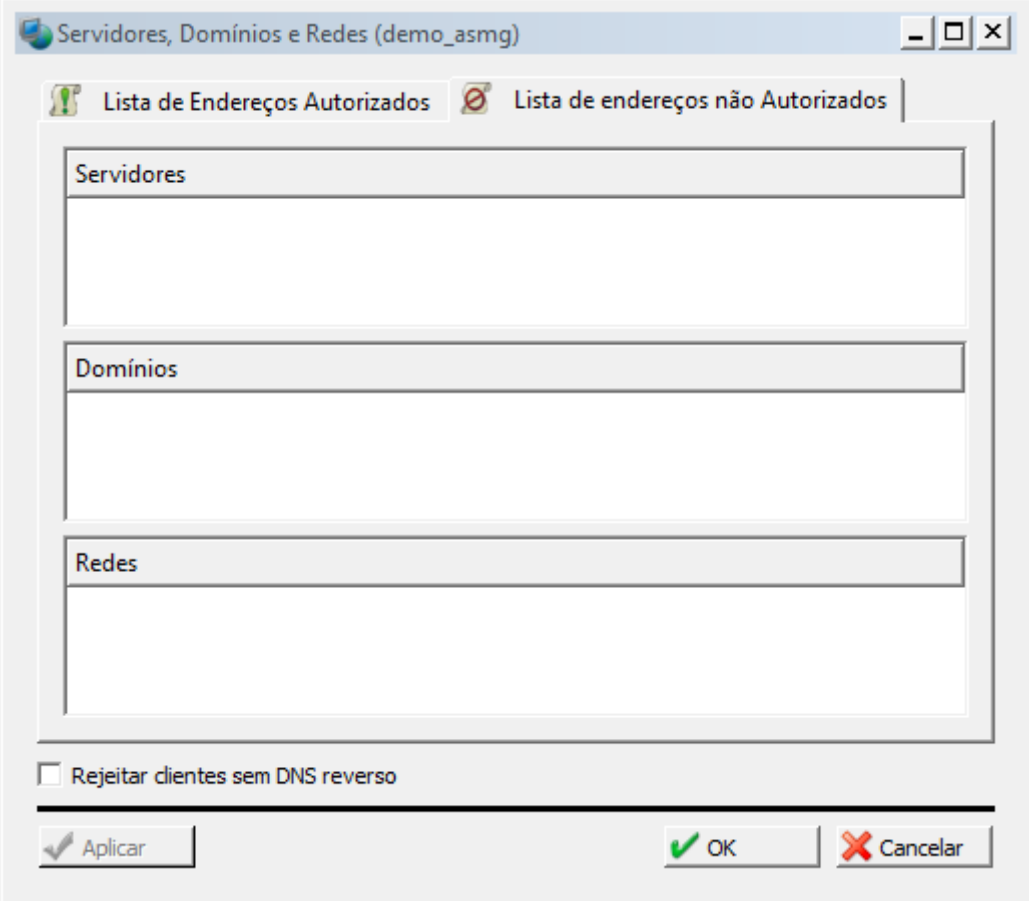

Figura 64. Lista de endereços não autorizados.

Para referenciar uma entidade do tipo "Servidor", "Domínio" ou "Rede", que deva ter sua conexão recusada, clicar com o botão direito do mouse sobre o respectivo quadro e escolher a opção **"Adicionar Entidades"**. A seguir, escolher a(s) entidade(s) cuja conexão deva ser bloqueada e clique em **"Adicionar"**.

A opção de "Domínios" incluirá na blacklist de conexões todos os servidores que tiverem parte do domínio escolhido por resolução de DNS Reverso**.**

Filtragem de E-mail

9. Filtragem de E-mail

O item **"Filtragem de E-mail**" compreende uma série de regras que serão aplicadas igualmente a todos os usuários de redes intermediadas pelo **ASMG**.

Desta maneira, as configurações feitas através deste item serão estendidas para todas as políticas e grupos que forem criados dentro do **ASMG**.

Esse item compreende as seguintes opções:

- Análise de Vírus;
- Análise de Remetente;
- Gray Listing;
- Regras Avançadas;
- Whitelist/Blacklist.

Análise de vírus

Nesta janela é possível habilitar a filtragem do **ASMG** no que diz respeito à integração com o servidor que contém o agente de antivírus. Sendo produtos diferentes, o **ASMG** envia todos os anexos existentes nas mensagens (tanto as enviadas quanto às recebidas) para o antivírus e depois analisa a sua resposta.

Aqui serão configuradas apenas as ações que devem ser tomadas caso um vírus seja encontrado e tipos de arquivos que devem ser ignorados na análise de vírus.

Aba Entrada

Esta aba refere-se às mensagens que chegam da Internet para um usuário que está dentro da área controlada pelo **ASMG**.

© Aker Security Solutions

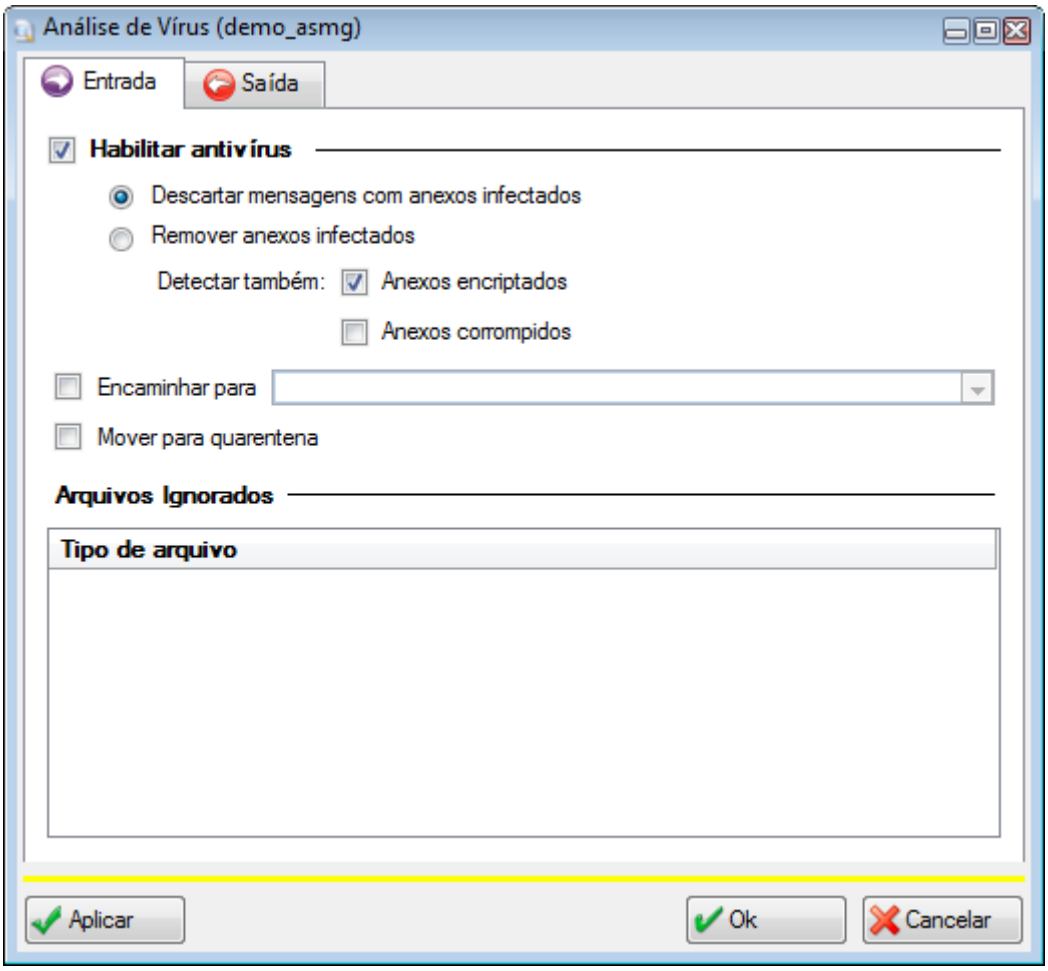

Figura 65. Análise de Virus - Entrada.

Contém as seguintes opções:

- **Habilitar Antivírus**

Se esta caixa de seleção for marcada, toda e qualquer mensagem com anexo que for recebida será analisada.

Caso o anexo esteja infectado, encriptado ou corrompido, é possível remover apenas o anexo e liberar a mensagem informando a remoção ou descartar a mensagem completamente.

É possível ainda encaminhar uma cópia da mensagem para o Administrador do sistema e movê-la, se desejar, para quarentena. Este tipo de comportamento favorece análises das mensagens infectadas e estudos de outras políticas que possam detectá-las.

© Aker Security Solutions

- **Arquivos ignorados**

Neste quadro tem-se a informação dos tipos de arquivos anexados que podem ser ignorados na análise do antivírus. Estes tipos de arquivos devem estar previamente cadastrados como entidades do tipo **"Arquivos".**

Para adicionar uma entidade do tipo **"Arquivo",** clicar com o botão direito do mouse no quadro **"Tipo de arquivo"**. Em seguida, selecionar **"Adicionar Entidades"** e escolher o tipo de arquivo que será ignorado. Depois, clicar em **"Adicionar"**. Podem ser escolhidos vários tipos de arquivo ao mesmo tempo.

- **Aba Saída**

Esta aba possui configuração igual à aba **"Entrada".** A principal diferença entre as duas é que os arquivos que serão examinados são aqueles enviados como anexo em alguma mensagem que vá de dentro da(s) área(s) controlada(s) pelo **ASMG** para a Internet.

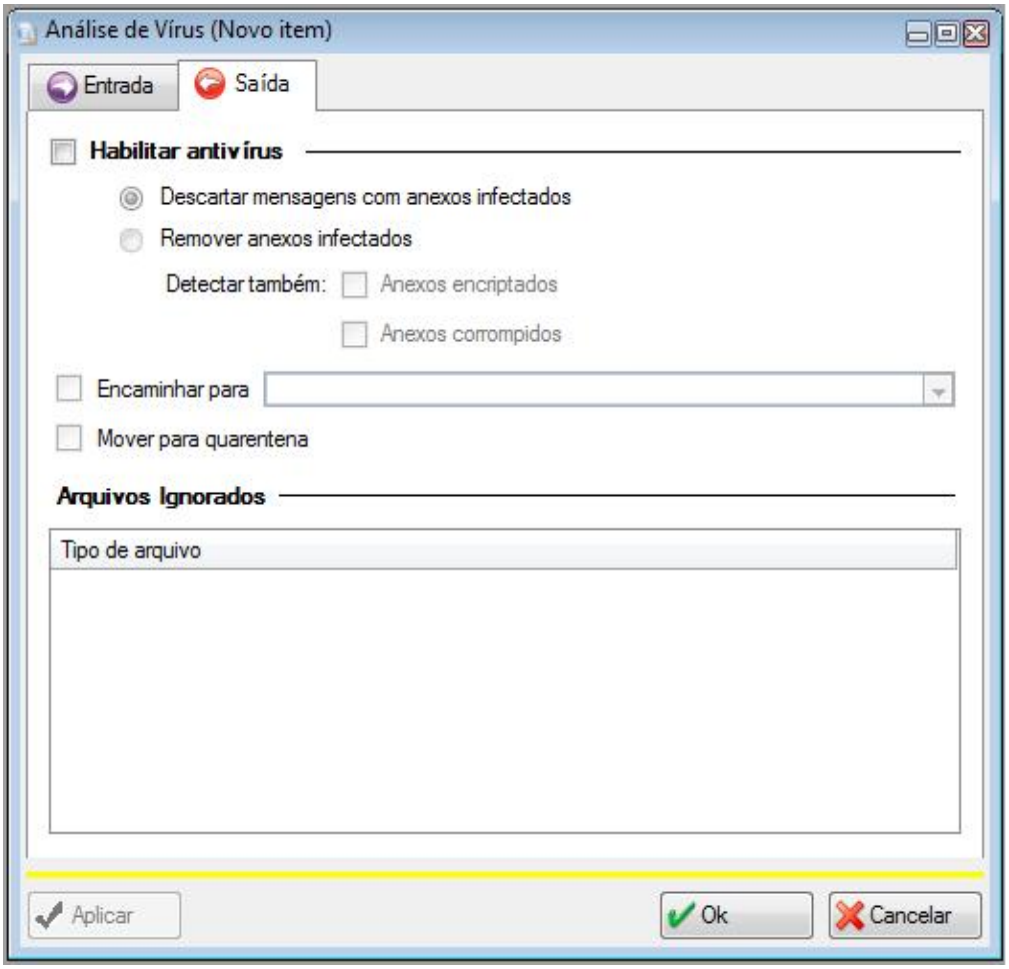

Figura 66. Análise de Virus - Saída.

Contém as seguintes opções:

- **Habilitar Antivírus**

Se esta caixa de seleção for marcada, toda e qualquer mensagem enviada que contiver anexo será analisada.

Caso o anexo esteja infectado, encriptado ou corrompido, é possível remover apenas o anexo e liberar a mensagem informando que o anexo foi removido ou descartar a mensagem completamente. Também é possível encaminhar uma cópia da mensagem para o Administrador do sistema e movê-la, se desejar, para quarentena. Este tipo de comportamento favorece análises das mensagens infectadas e estudos de outras políticas que possam detectá-las.

- **Arquivos ignorados**

Este quadro informa os tipos de arquivos anexados que podem ser ignorados na análise do antivírus. Estes tipos de arquivos devem ser previamente cadastrados como entidades do tipo **"Arquivos"**.

Para adicionar uma entidade do tipo **"Arquivo",** é necessário clicar com o botão direito do mouse no quadro **"Tipo de arquivo"**. Em seguida, selecionar a opção **"Adicionar Entidades"** e escolher o tipo de arquivo que será ignorado. Depois, clicar em **"Adicionar"**.

Análise do Remetente/Destinatário

Habilitar checagem de remetente

A checagem é realizada durante a negociação de uma mensagem, ao receber a informação sobre quem é o remetente, o **ASMG** conecta-se em algum servidor MX responsável pelo domínio indicado no cabeçalho da mensagem original e verifica se o remetente fornecido é reconhecido por este último. Em caso positivo, a mensagem é aceita. Em caso negativo, ela é rejeitada.

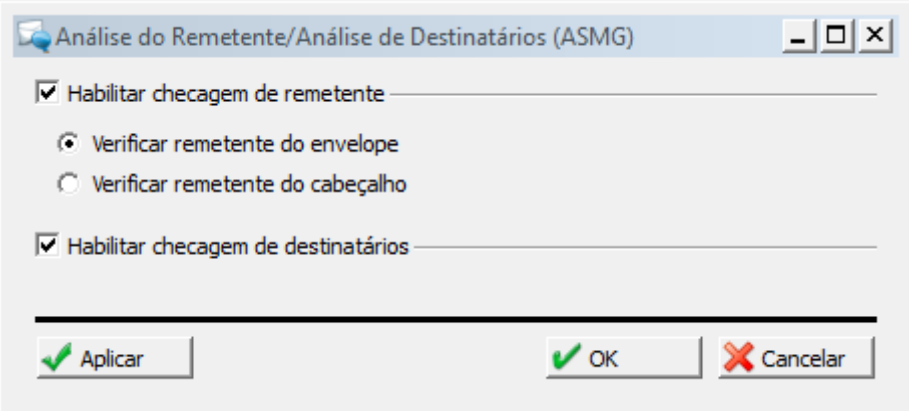

Figura 67. Análise do remente/Análise dos destinatários.

Esta funcionalidade busca combater Spams, uma vez que grande parte destas mensagens utiliza remetentes inválidos ou não existentes. A análise pode ser feita tanto pelo cabeçalho da mensagem quanto pelo remetente mencionado no envelope, bastando selecionar a opção adequada.

Habilitar checagem de destinátarios

A checagem é realizada durante a negociação de uma mensagem, ao receber a informação sobre quem são os destinatários, o **ASMG** conecta-se nos servidores protegidos por ele pelo domínio indicado no envelope da mensagem original e verifica se o destinatário fornecido existe. Em caso positivo, a mensagem é aceita. Em caso negativo, ela é rejeitada.

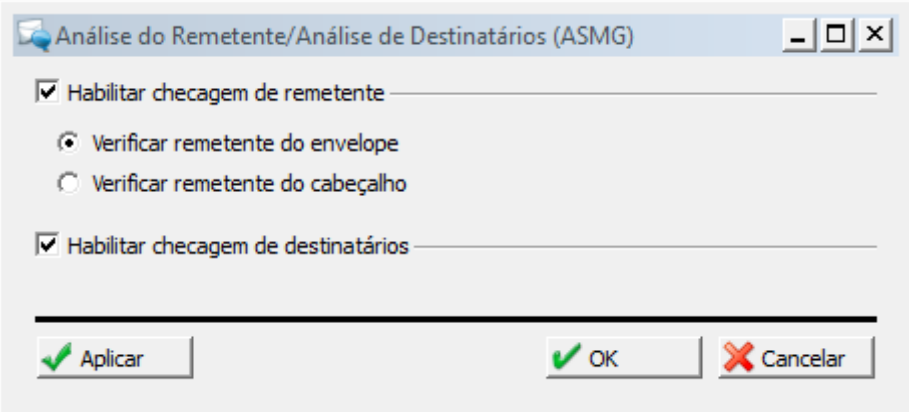

Figura 68. Análise do remente/Análise de destinatários.

Gray Listing

Este é um método simples para defender as caixas de e-mail dos usuários contra spammers. Quando habilitada, faz com que o sistema rejeite qualquer mensagem vinda de um remetente desconhecido, especificando um erro temporário.

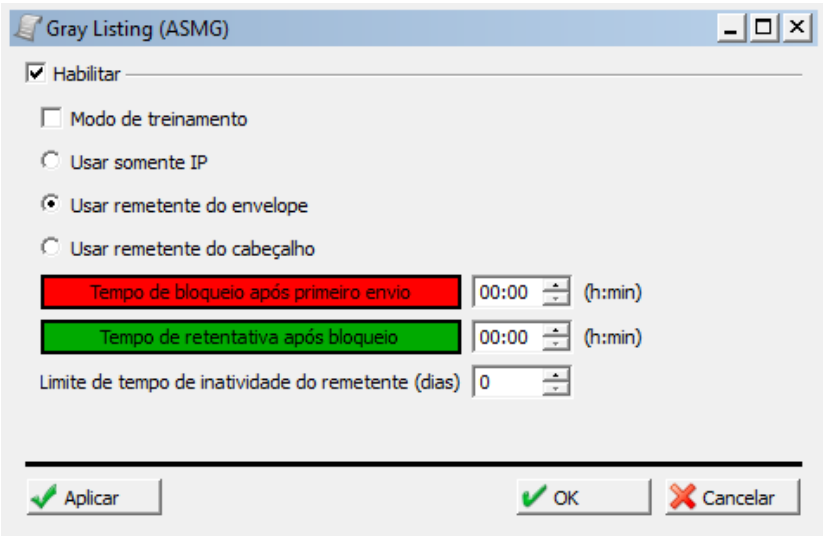

Figura 69. Gray listing.

Pela designação do protocolo SMTP, quando um cliente não consegue enviar uma mensagem para o servidor de destino por motivo de erro temporário, ele deve continuar tentando o envio por aproximadamente cinco dias. Ao final deste prazo, a mensagem é descartada e o remetente avisado do insucesso. Baseado nesta idéia, o **ASMG** simula um erro temporário de conexão para que a mensagem não possa ser entregue pelo cliente. Se a mensagem for legítima, o cliente tentará nova conexão posteriormente e, nesta nova tentativa, o sistema aceitará o e-mail.

O **ASMG** parte da premissa que se o e-mail é de um spammer, provavelmente não haverá uma nova tentativa de envio. Isso acontece porque spammers normalmente utilizam robôs para o envio de mensagens em massa e muito dificilmente reenviam essas mensagens que acusaram erro. Dentre as configurações possíveis no processo de análise o Administrador pode escolher se o que será considerado para análise será: o remetente do envelope, ou o remetente do cabeçalho ou somente o IP.

A opção **"Tempo de Bloqueio"** refere-se ao tempo mínimo, em horas, que deve se passar entre a primeira e a segunda tentativa de negociação para o envio da mensagem. Durante esse período o sistema rejeitará todas as tentativas de negociação de envio.

O Administrador também pode configurar o **"Tempo de nova tentativa"**, que é o tempo em horas, depois de terminado o tempo de bloqueio, que o sistema aguarda pela segunda tentativa de negociação para o envio da mensagem.

Se a segunda tentativa for realizada dentro deste tempo, o remetente será considerado autêntico e inserido na lista de endereços autorizados.

Uma vez dentro da lista de endereços autorizados, o parâmetro **"Limite de tempo de inatividade do remetente"** define por quanto tempo (em dias) o usuário será mantido nesta lista. Sempre que uma nova mensagem do mesmo remetente for recebida, o limite de tempo de inatividade é renovado.

Modo de treinamento

Quando o ASMG é recém instalado, a base de Graylist está vazia e isso faz com que todos os e-mails sejam bloqueados. Para ocorrer à redução desse bloqueio foi criado o modo de treinamento que adiciona as informaçãoes (endereço IP, endereço do remetente/destinatário), na lista de endereços autorizados sem realizar o bloqueio. Após o modo de treinamento ser desabilitado, o filtro passa a funcionar normalmente, bloqueando quem não está na lista de e-mails.

© Aker Security Solutions

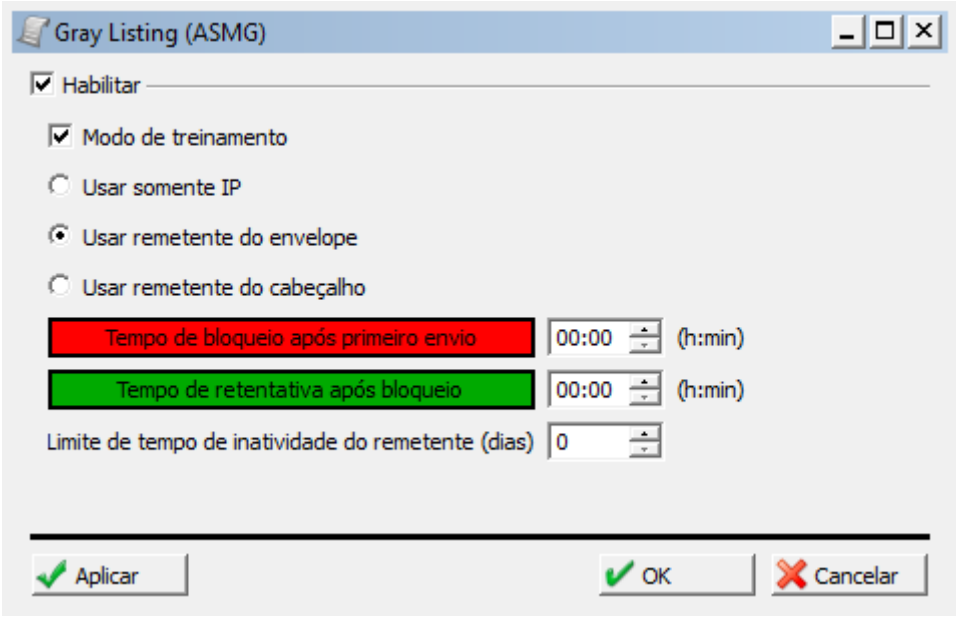

Figura 70. Gray listing – modo de treinamento.

Regras Avançadas

Na implementação atual do **ASMG**, as regras de filtragem são criadas automaticamente quando o usuário clica sobre as respectivas telas e escolhe uma ação a ser executada. Ainda assim, pode ocorrer de as regras dinâmicas não serem suficientes para atender a alguma demanda específica e, nesses casos, há a opção de criar as regras manualmente.

Composta pelas abas **"Pré-regras"** e **"Pós-regras"**, esta janela deve ser utilizada por usuários avançados a fim de se especificar regras que não possam ser automaticamente geradas através das janelas de filtragem oferecidas pela interface gráfica. Na prática, todas as filtragens efetuadas pelo **ASMG** são interpretadas como regras. Contudo, a sintaxe destas regras é de alta complexidade para a compreensão/manipulação corriqueira.

A diferença entre as pré e as pós regras é o momento de execução das mesmas. As pré-regras são executadas antes das regras convencionais geradas automaticamente pelo sistema. As pós-regras são executas após as regras convencionais.

© Aker Security Solutions

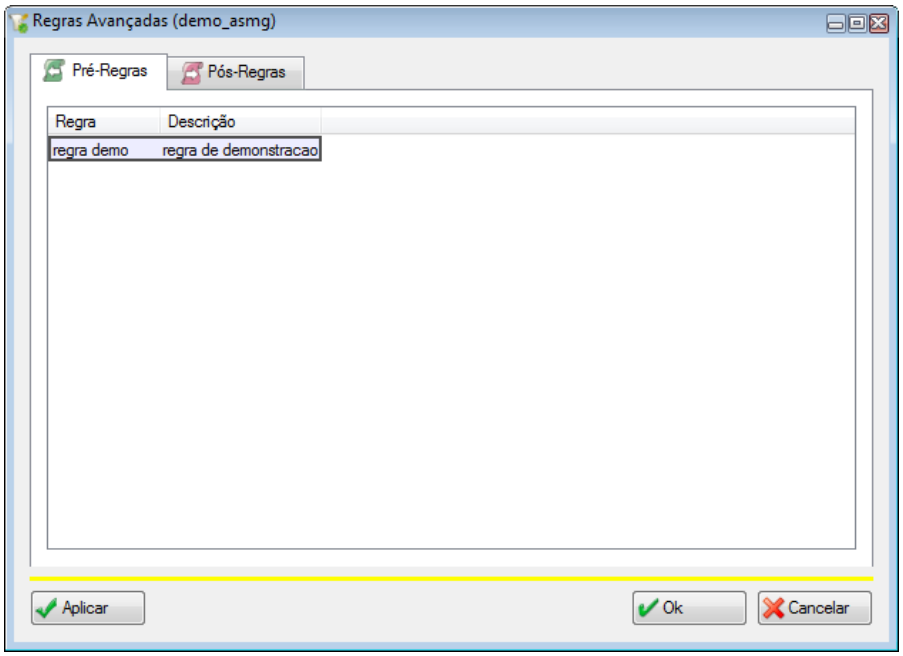

Figura 71. Regras avançadas – Pré-regras.

Whitelist/Blacklist

Esta configuração definirá quais e-mails ou domínios farão parte de uma whitelist ou blacklist. Isto significa que o e-mail/domínio que estiver em uma whitelist não será bloqueado por nenhum filtro de nenhuma política e o e-mail/domínio que estiver em uma blacklist será bloqueado.

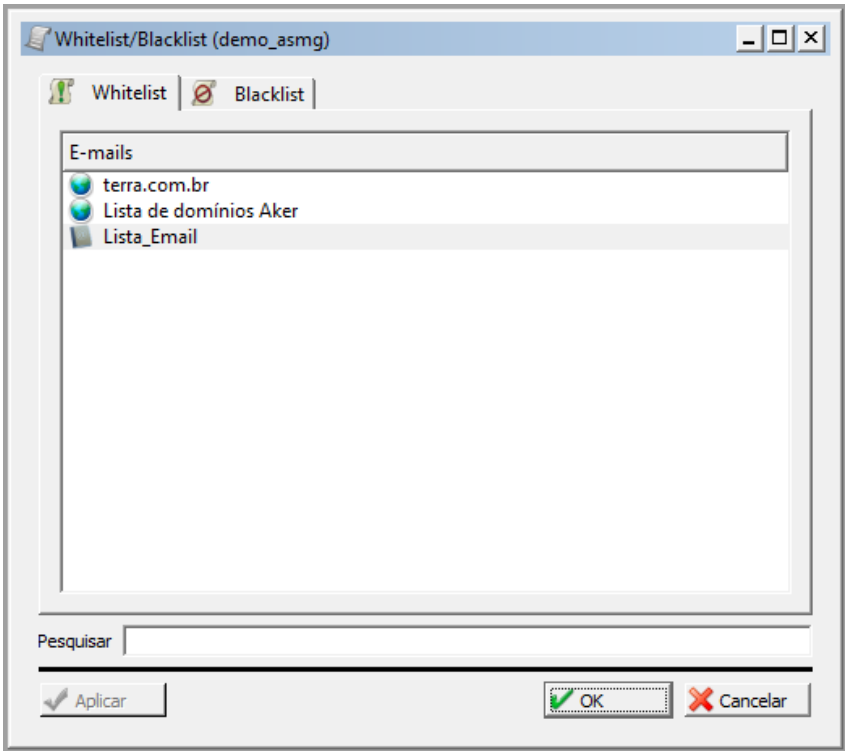

Figura 72. Whitelist/Blacklist.

Informação do Sistema

10. Informação do Sistema

Esta subárvore guarda as janelas relacionadas à informação do sistema, tais como memória consumida, em todos os níveis, e estado do processador do servidor onde está instalado o ASMG. Aqui também fica a janela que apresenta mensagens atualmente em processamento pelo ASMG, em níveis de recebimento, processamento e envio.

Fila de Trabalho

Esta janela informa quais são as mensagens que estão atualmente sendo processadas pelo sistema em três diferentes situações: na entrada, no processamento e no encaminhamento.

Aba Recebendo

Mostra as mensagens que estão sendo recebidas pelo **ASMG**. Nesta tela pode-se visualizar o status de recebimento da mensagem pelo servidor, e o endereço IP do cliente.

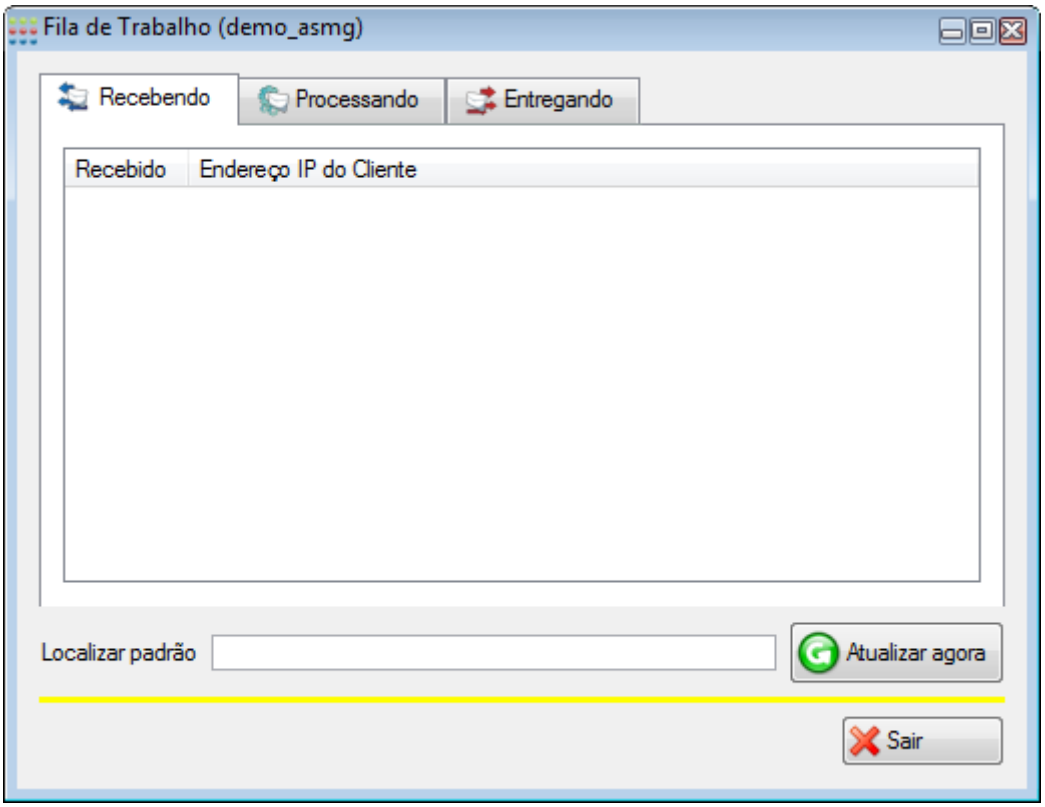

Figura 73. Fila de trabalho - recebendo.

Devido ao alto desempenho do sistema, é comum esta janela não apresentar dados. Ela só deve apresentar dados em casos de sistema trabalhando em picos de processamento.

Aba Processando

Esta aba mostra as mensagens que estão sendo processadas pelo **ASMG**. Nela visualiza-se as informações sobre o recebimento da mensagem, remetente e destinatário.

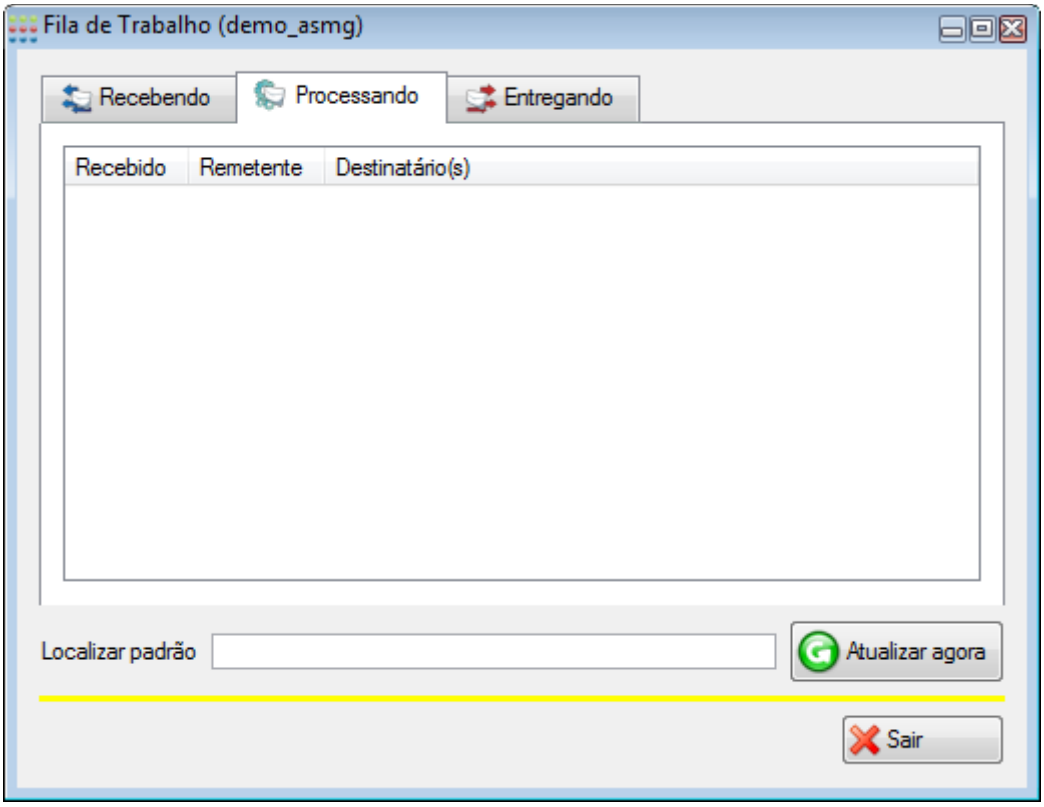

Figura 74. Fila de trabalho - processando.

Devido ao alto desempenho do sistema é comum esta janela não apresentar dados. Ela só deve apresentar dados em casos de sistema trabalhando em picos de processamento.

Aba Entregando

Esta aba mostra as mensagens que estão sendo entregues pelo **ASMG**. Nela pode-se visualizar se a mensagem foi recebida, quem a enviou, quem a recebeu, prazo final para entrega, número de tentativas de entrega e, caso haja, o motivo de adiamento.

© Aker Security Solutions

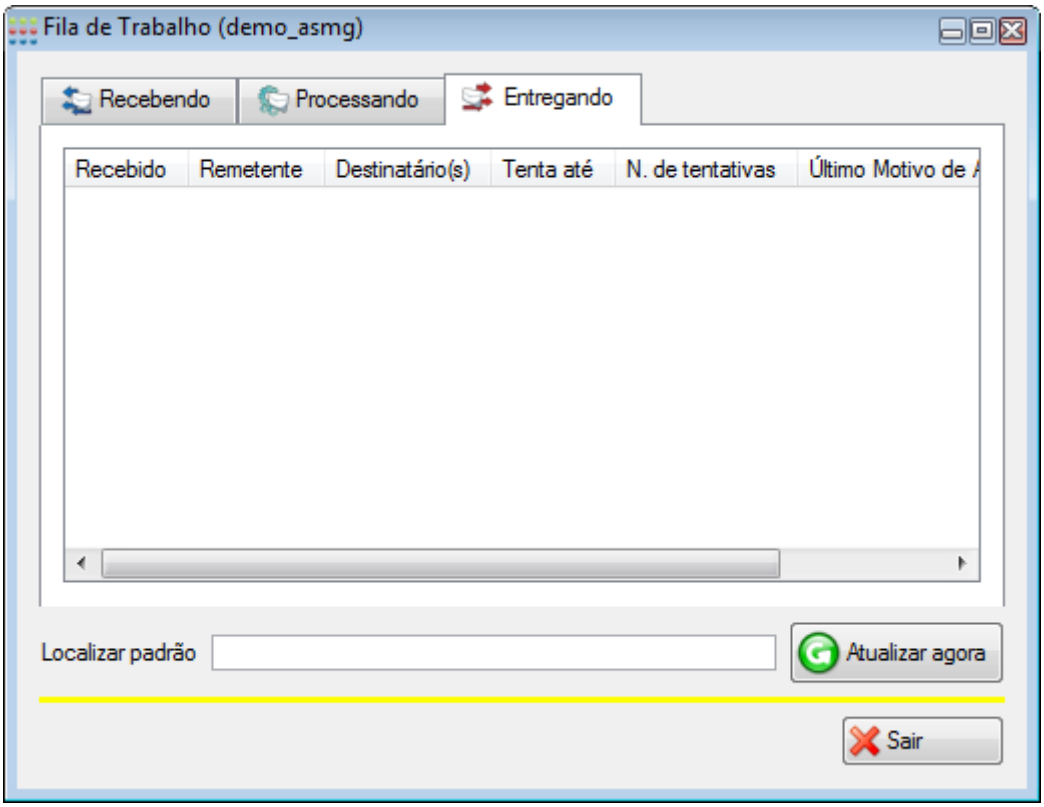

Figura 75. Fila de trabalho - entregando.

Nesta janela é comum existirem muitas mensagens sendo mostradas. Elas representam todas as mensagens que, devido a algum erro temporário, ainda não foram entregues pelo ASMG ao servidor de e-mail de destino.

Sempre que o sistema de confirmação estiver habilitado, aparecerão aqui também as mensagens ainda não confirmadas.

Status do Sistema

Nesta janela é mostrada, numericamente, a taxa de utilização do processador naquele momento exato. Além disso, há mostradores digitais informando a quantidade de memória livre, a quantidade de memória em uso e/ou a taxa de utilização da memória cache.

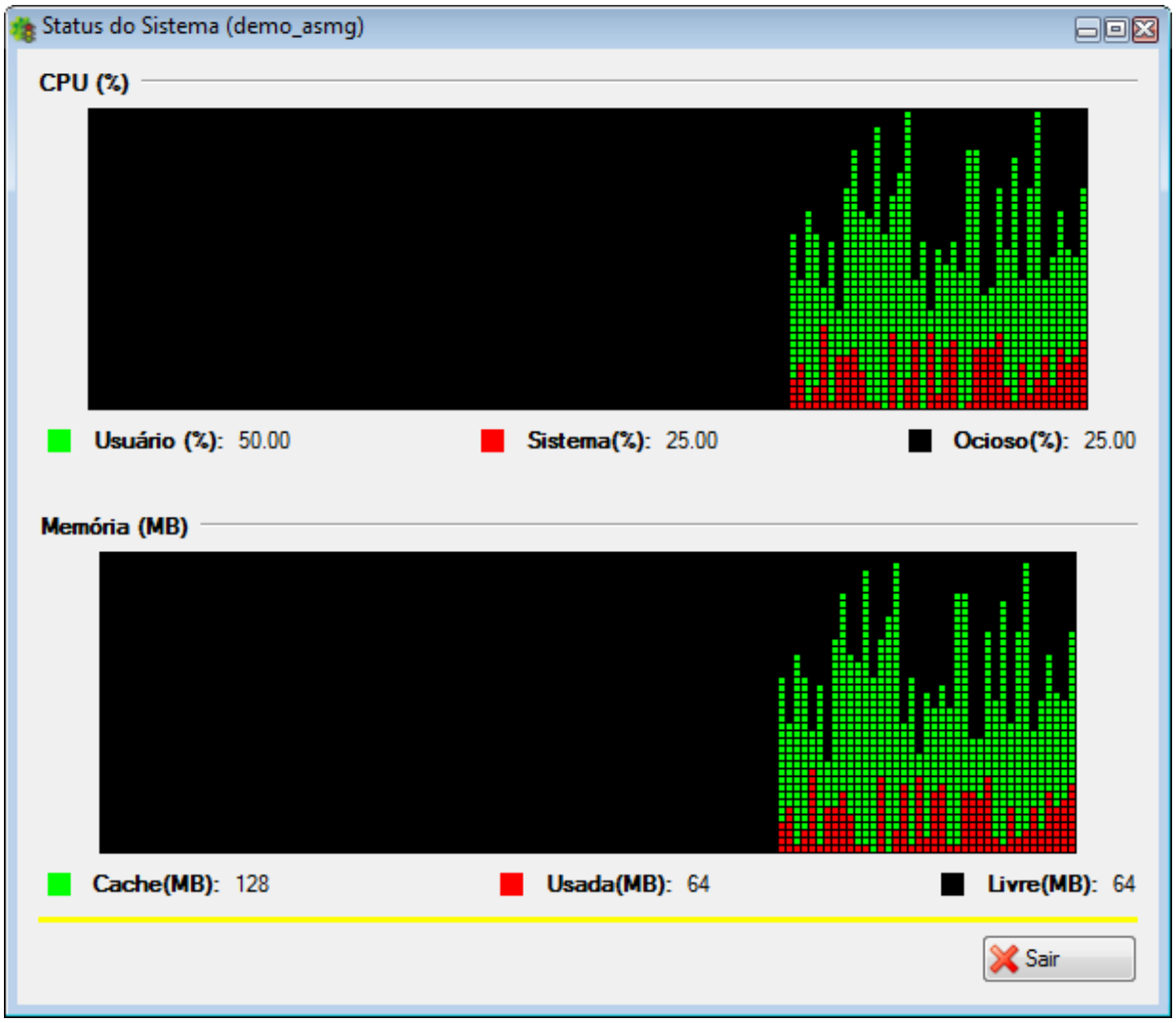

Figura 76. Status do sistema.

© Aker Security Solutions

Logs

11. Logs

Esta subárvore guarda as janelas relacionadas ao gerenciamento, visualização e controle dos registros de controle do produto, também conhecidos por logs. É composta por duas partes:

- Configurações de log;
- Visualizador de log.

Configurações de Log

Esta é a janela que cuida das configurações relativas à geração, tratamento e armazenamento dos arquivos de log do ASMG. Ela está dividida em duas abas:

Aba de Configurações Gerais

Aba com as configurações dos logs. É composto das seguintes opções:

- Caminho Arquivos Log

Local (diretório no disco rígido) onde serão armazenados os arquivos de log gerados pelo produto.

- Tamanho Máximo

Especifica o tamanho máximo do arquivo de log que irá ser armazenado pelo produto. Pode ser selecionada a opção **"Desabilita Tamanho Máximo"** para desabilitar essa função.

- Período de Armazenamento

Especifica por quanto tempo (dias ou horas) que o produto irá armazenar as informações de log. Pode ser selecionada a opção **"Desabilita Período de Armazenamento"** para desabilitar essa função.

- Freqüência de Rotação

Especifica a freqüência de geração de arquivos de log para um mesmo dia. Por exemplo, se o número selecionado for 24, será gerado um arquivo de log para cada hora do dia.

- Logar no sistema

© Aker Security Solutions

Caso seja marcado, essa opção irá gravar arquivos de logs idênticos no sistema de log do sistema operacional (Syslog do Linux).

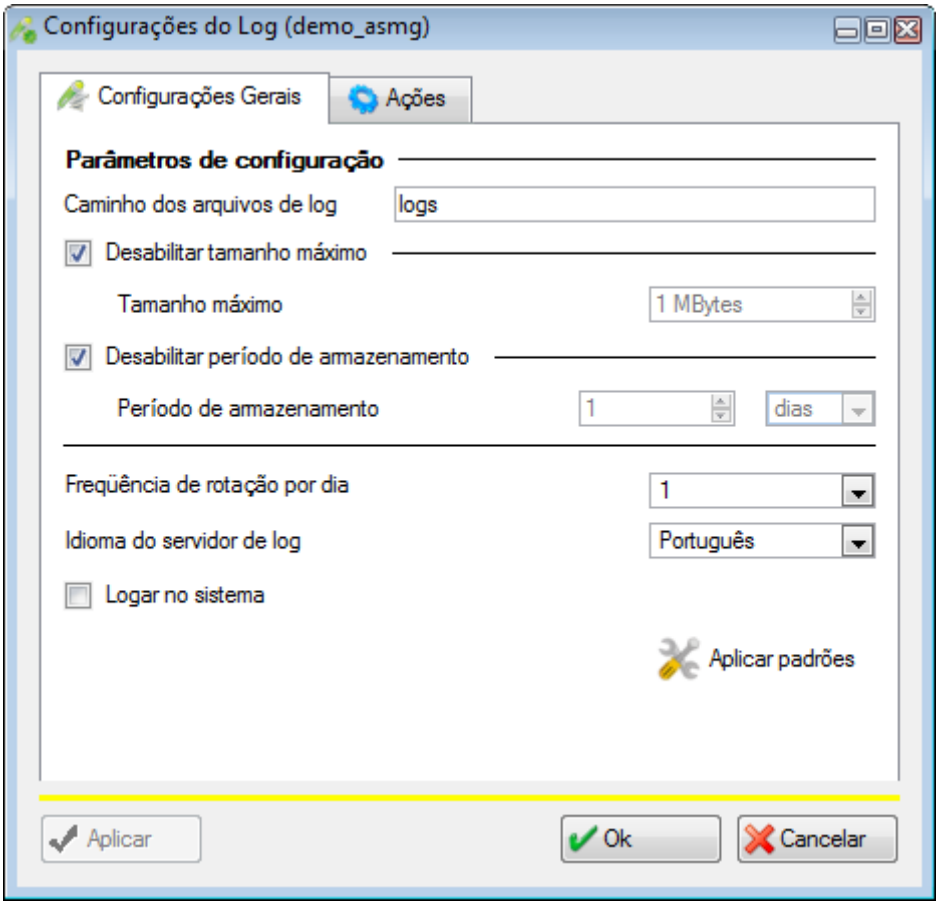

Figura 77. Configurador de log – configurações gerais.

O administrador deve ter bastante atenção ao configurar essas opções sempre lembrando que o dispositivo de armazenamento utilizado tem um limite físico de tamanho e que alguns sistemas operacionais não conseguem trabalhar com arquivos de formatos muito grandes.

Aba de Ações

A aba de ações apresenta todas as mensagens de log existentes e relaciona cada uma delas ao produto gerador. Também é possível escolher quais das mensagens existentes devem ser logadas.

Exportações Agendadas

Os registros de Logs e Eventos são exportados nos formatos TXT, publicados via FTP, E-mail ou localmente em uma pasta do próprio ASMG. Podem ser agendados das seguintes formas: "Diário", "Semanal" e/ou “Mensal”.

Para ter acesso à janela de Exportação Agendada deve-se:

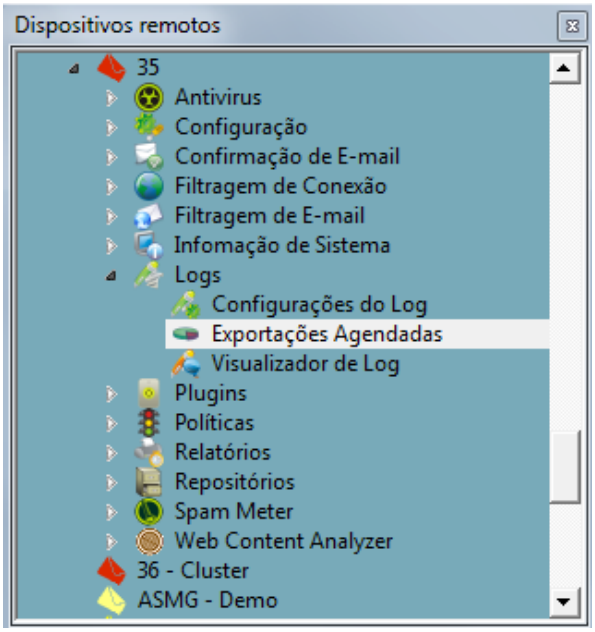

Figura 78. Janela de acesso: Exportações agendadas.

- Clicar no menu *Logs* da janela de administração do Aker Secure Mail Gateway;
- Selecionar o item *Exportações Agendadas*.

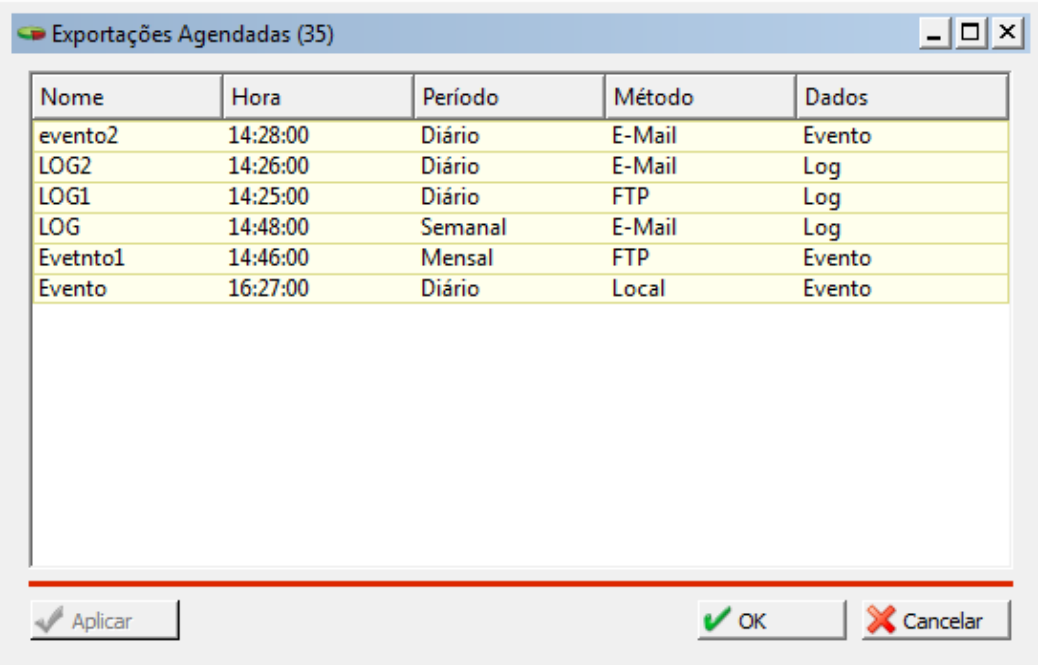

Figura 79. Exportações agendadas.

Para executar qualquer exportação, deve-se clicar com o botão direito do mouse sobre ele. Aparecerá o seguinte menu: (este menu será acionado sempre que for pressionado o botão direito, mesmo que não exista nenhum relatório selecionado. Neste caso, somente as opção *Inserir* estará habilitada); inclusive podendo ser executada a partir da barra de ferramentas.

- **Inserir:** Esta opção permite incluir um novo agendamento.

© Aker Security Solutions

Opções de agendamentos

Nesta aba serão configurados os seguintes campos:

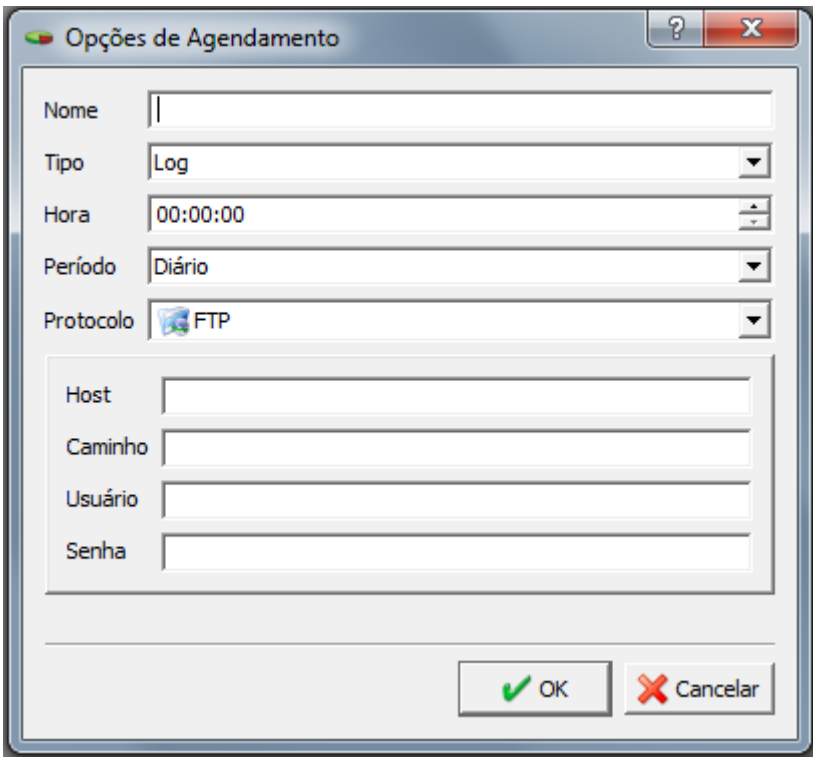

Figura 80. Opções de agendamentos.

- **Nome:** Atribuir nome a exportação;
- **Tipo:** Define qual informação será exportada:
  - Log;
  - Eventos.
- **Hora:** Definir hora que será realizada a exportação;
- **Período:** Definir a freqüência que será realizada a exportação:
  - Diário;
  - Semanal;
  - Mensal.
- **Protocolo:** Definir o método que será realizado a exportação:
  - FTP - o usuário poderá indicar até três servidores para onde serão enviados os dados via ftp;
  - E-mail – endereço do e-mail que deseja enviar as informações exportadas;
  - Local - o usuário poderá indicar em qual pasta local do Aker Secure Mail Gateway deseja salvar os dados exportados.

© Aker Security Solutions

Visualizador de logs

Esta janela controla a visualização dos dados de log do **ASMG**. Existem dois tipos de logs:

- Mensagens - que armazena todos os dados de relevância de uma mensagem, tais como remetente, destinatário, tamanho máximo, IP do cliente, nome do cliente;
- Eventos - que armazena fatos de importância ocorridos durante o processamento das mensagens pelo sistema.

É possível ainda especificar filtros para obtenção de dados de log. As janelas de parâmetros disponíveis são diferentes para os logs de mensagens e de eventos, mas alguns são comuns a ambos.

Logs de Mensagens

Visualiza o resultado do processamento de todas as mensagens que passaram pelo **ASMG**.

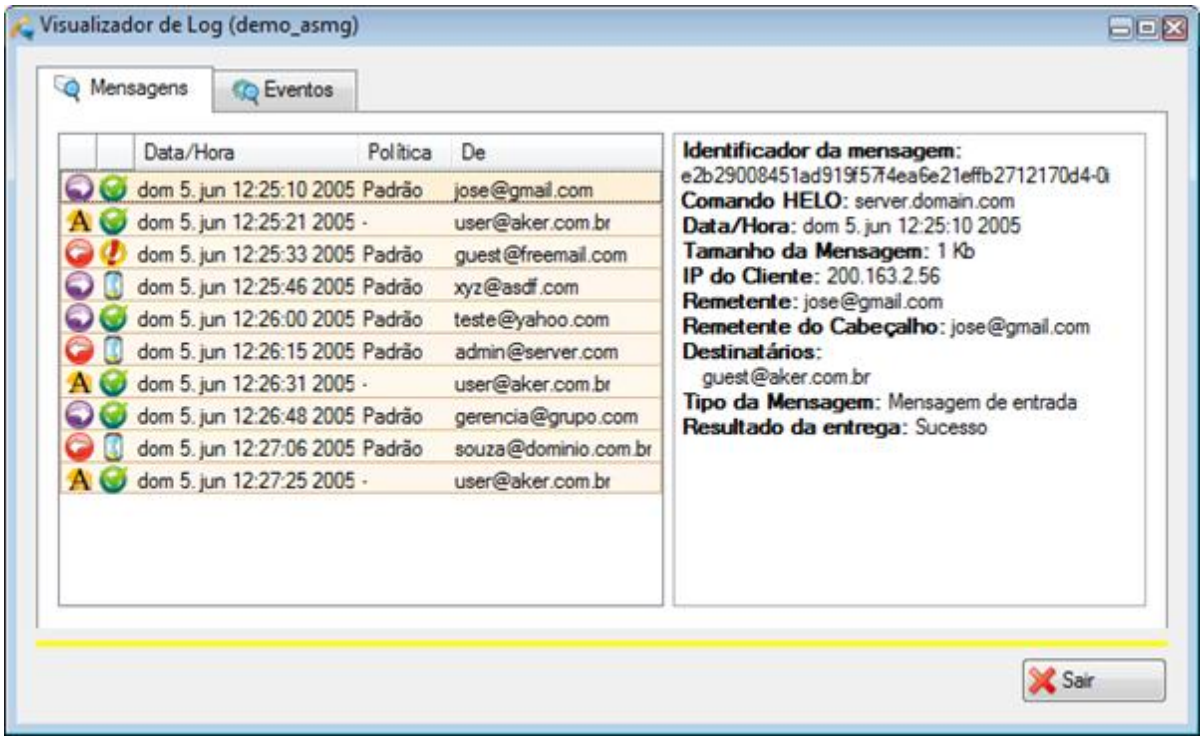
Visualizador de Log (demo_asmg)
Mensagens
Eventos
Data/Hora
Política
De
dom 5. jun 12:25:10 2005 Padrão jose@gmail.com
dom 5. jun 12:25:21 2005 - user@aker.com.br
dom 5. jun 12:25:33 2005 Padrão guest@freemail.com
dom 5. jun 12:25:46 2005 Padrão xyz@asdf.com
dom 5. jun 12:26:00 2005 Padrão teste@yahoo.com
dom 5. jun 12:26:15 2005 Padrão admin@server.com
dom 5. jun 12:26:31 2005 - user@aker.com.br
dom 5. jun 12:26:48 2005 Padrão gerencia@grupo.com
dom 5. jun 12:27:06 2005 Padrão souza@dominio.com.br
dom 5. jun 12:27:25 2005 - user@aker.com.br
Identificador da mensagem: e2b29008451ad919f57f4ea6e21effb2712170d4-0i
Comando HELO: server.domain.com
Data/Hora: dom 5. jun 12:25:10 2005
Tamanho da Mensagem: 1 Kb
IP do Cliente: 200.163.2.56
Remetente: jose@gmail.com
Remetente do Cabeçalho: jose@gmail.com
Destinatários:
guest@aker.com.br
Tipo da Mensagem: Mensagem de entrada
Resultado da entrega: Sucesso
Sair

Figura 81. Visualizador de log.

Dentre as informações relativas ao processamento de cada mensagem, existe um parâmetro que mostra o resultado de entrega. Existem quatro possíveis resultados. São eles:

- Sucesso: a mensagem foi entregue satisfatoriamente ao destinatário;
- Fracasso: houve um erro permanente na tentativa de entrega;

© Aker Security Solutions

- Bloqueio: a mensagem não foi entregue porque foi bloqueada por algum filtro configurado pelo usuário;
- Desistência: ocorre após cinco dias de tentativa de entrega sem sucesso (nesse caso a mensagem é descartada).

Quando uma mensagem é selecionada no quadro à esquerda, todos os dados de relevância referentes a ela são mostrados no quadro da direita.

Filtros do Log de Mensagens

Para facilitar a busca, é possível ainda filtrar as mensagens de acordo com os seguintes parâmetros:

- Intervalo de data e hora (início e fim);
- Remetente;
- Domínio do remetente;
- Remetente do Cabeçalho;
- Domínio do Remetente do Cabeçalho;
- Assunto;
- Destinatário;
- Identificador da mensagem (dado interno ao ASMG, inserido no header da mensagem como valor da tag X-AkerSMTPGW-MessageID);
- Resultado da Entrega (sucesso, fracasso, bloqueio ou desistência);
- Tipo de mensagem (entrada, saída, interna ou de sistema).

© Aker Security Solutions

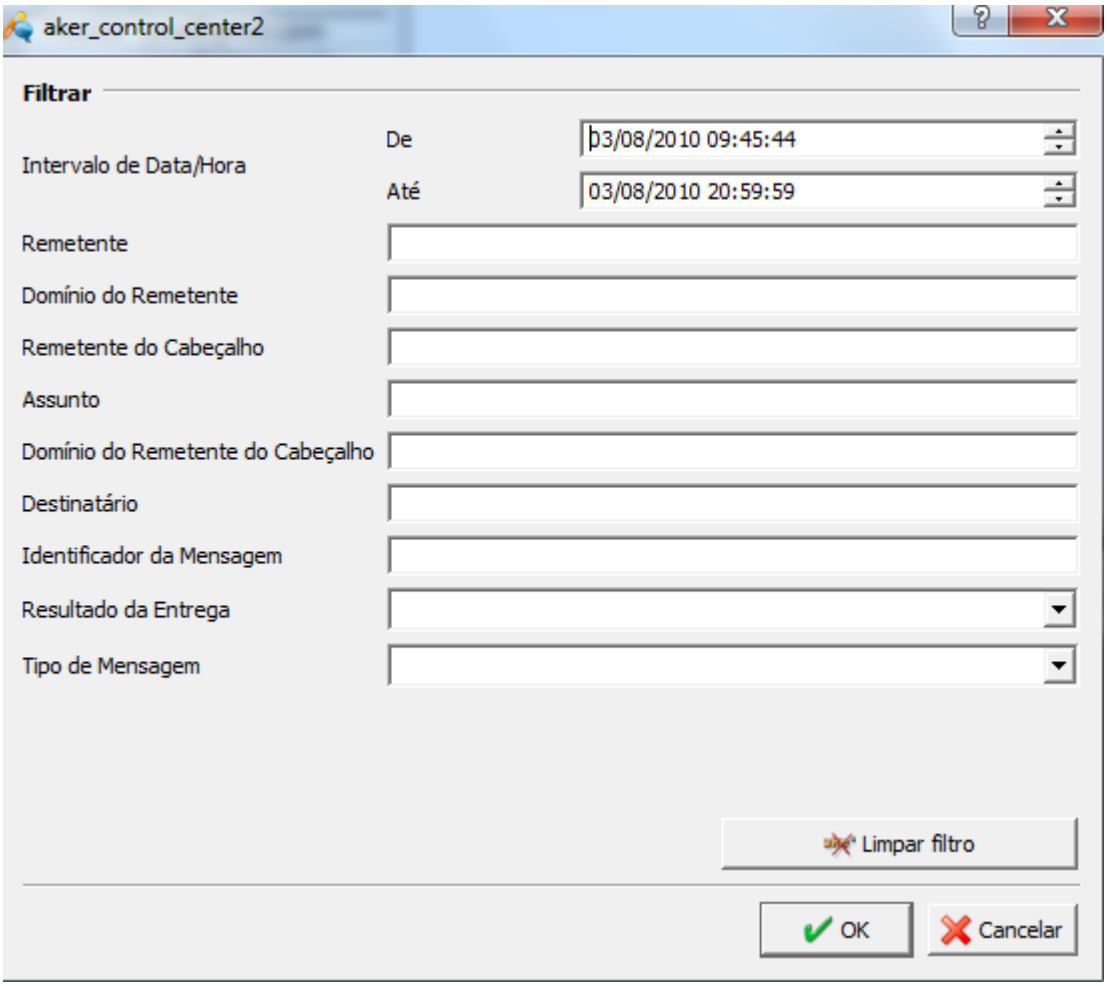

Figura 82. Filtro de log de mensagens.

Para ter acesso ao filtro, basta clicar sobre o botão **"Filtrar"**, disponível na barra de ferramentas do **Aker Control Center.**

As mensagens processadas pelo ASMG só receberão um log de mensagem quando tiverem seu ciclo de vida encerrado no produto, ou seja, quando tiverem sido enviadas ao servidor de destino ou então quando tiverem tido bloqueio, erro permanente ou desistência na entrega. Algumas mensagens podem, portanto, levar até 5 dias para terem um log de envio, contados a partir do momento em que o ASMG a recebeu. Em casos de erro temporário de entrega, as mensagens ficam armazenadas na fila de saída, podendo ser visualizadas a partir da janela de fila de trabalho.

Logs de Eventos

Eventos são, no contexto do ASMG, acontecimentos de relevância ocorridos durante a execução do produto. Os eventos podem ou não estar relacionados a uma mensagem. Por exemplo, o evento de detecção de vírus em determinado anexo está diretamente relacionado ao processamento de uma mensagem. Já o erro na conexão com o agente de antivírus é um evento que não está relacionado a uma mensagem especificamente, mas sim ao ciclo de execução do **ASMG**.

© Aker Security Solutions

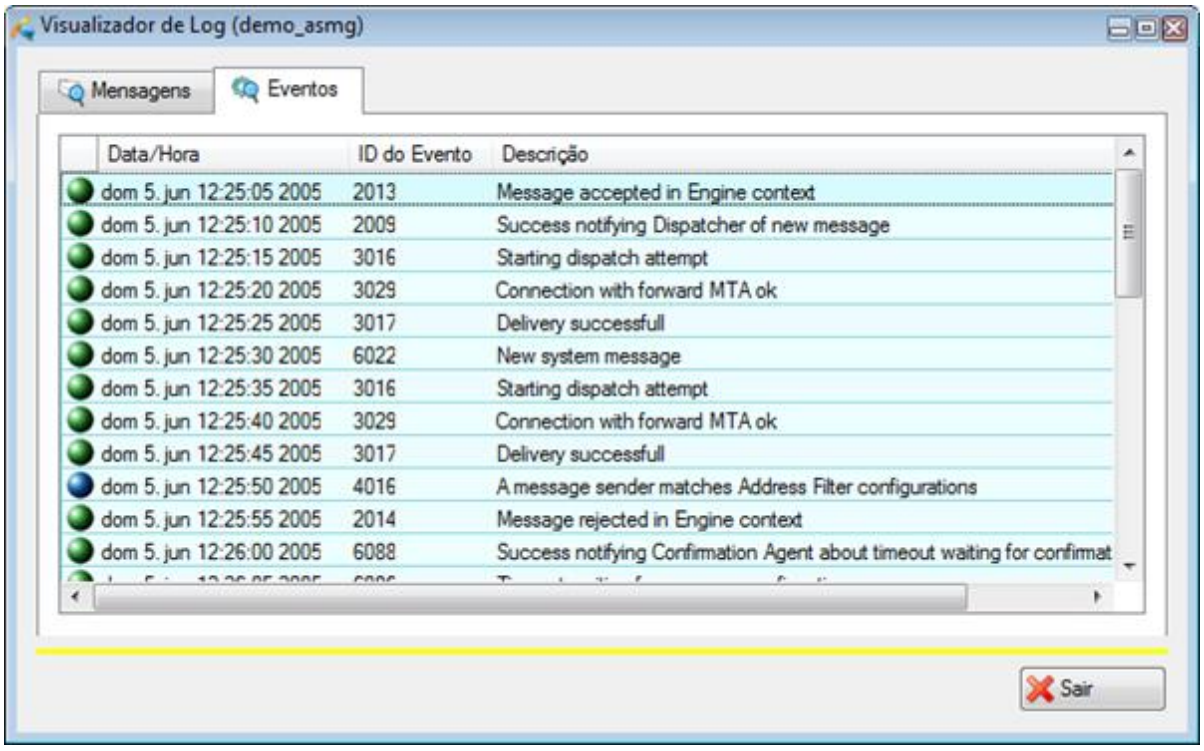
Visualizador de Log (demo_asmg)
Mensagens
Eventos
Data/Hora
ID do Evento
Descrição
dom 5. jun 12:25:05 2005 2013 Message accepted in Engine context
dom 5. jun 12:25:10 2005 2009 Success notifying Dispatcher of new message
dom 5. jun 12:25:15 2005 3016 Starting dispatch attempt
dom 5. jun 12:25:20 2005 3029 Connection with forward MTA ok
dom 5. jun 12:25:25 2005 3017 Delivery successfull
dom 5. jun 12:25:30 2005 6022 New system message
dom 5. jun 12:25:35 2005 3016 Starting dispatch attempt
dom 5. jun 12:25:40 2005 3029 Connection with forward MTA ok
dom 5. jun 12:25:45 2005 3017 Delivery successfull
dom 5. jun 12:25:50 2005 4016 A message sender matches Address Filter configurations
dom 5. jun 12:25:55 2005 2014 Message rejected in Engine context
dom 5. jun 12:26:00 2005 6088 Success notifying Confirmation Agent about timeout waiting for confirmat
Sair

Figura 83. Visualizador de log - eventos.

Nesta tela pode-se verificar a prioridade (primeira coluna), data e hora do evento, código de identificação do evento (ID), descrição do evento e detalhes referente ao item especificamente.

A prioridade define a gravidade do evento, ou seja, o quanto pode impactar no funcionamento do produto. Existem os seguintes tipos de prioridades:

- **Informação:** é atribuída a itens de log meramente informativos;
- **Aviso:** indica um item de log que representa um erro pequeno, que não impediu a entrega de mensagens;
- **Erro:** representa um erro que impediu o processamento/entrega de pelo menos uma mensagem;
- **Crítica:** representa um evento capaz de fazer o **ASMG** parar de funcionar;
- **Depuração:** representa eventos que podem ser utilizadas para a depuração do programa.

Nesta janela pode-se efetuar o treinamento de mensagens como SPAM ou HAM (Não SPAM) quando integrado com o Aker Spam Meter. Ao selecionar a linha de evento com o ID 4039, ficarão visíveis dois botões: SPAM e HAM como na imagem abaixo:

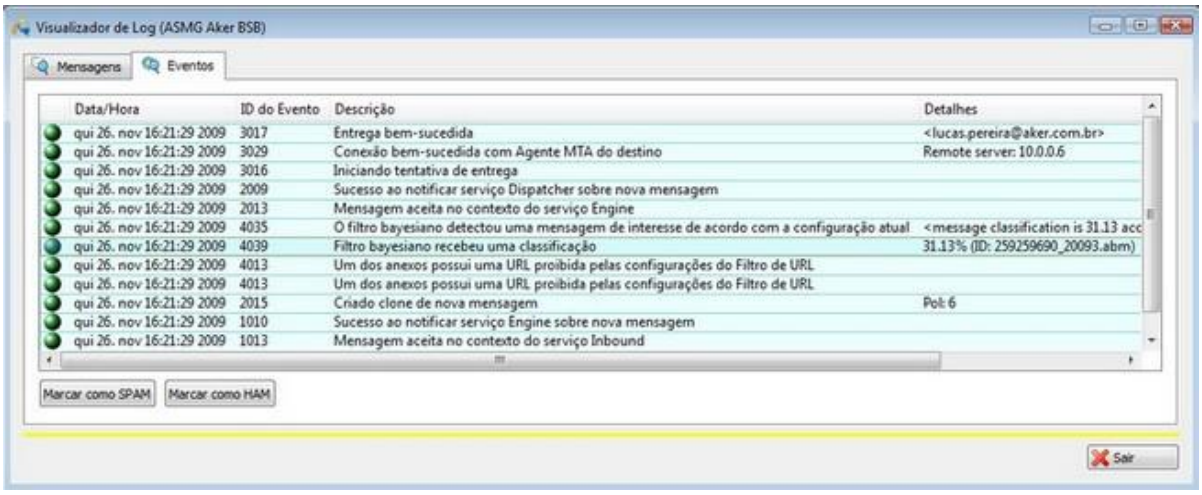
Visualizador de Log (ASMG Aker BSB)
Mensagens
Eventos
Data/Hora
ID do Evento
Descrição
Detalhes
qui 26. nov 16:21:29 2009 3017 Entrega bem-sucedida <lucas.pereira@aker.com.br>
qui 26. nov 16:21:29 2009 3029 Conexão bem-sucedida com Agente MTA do destino Remote server: 10.0.0.6
qui 26. nov 16:21:29 2009 3016 Iniciando tentativa de entrega
qui 26. nov 16:21:29 2009 2009 Sucesso ao notificar serviço Dispatcher sobre nova mensagem
qui 26. nov 16:21:29 2009 2013 Mensagem aceita no contexto do serviço Engine
qui 26. nov 16:21:29 2009 4035 O filtro bayesiano detectou uma mensagem de interesse de acordo com a configuração atual <message classification is 31.13 acc
qui 26. nov 16:21:29 2009 4039 Filtro bayesiano recebeu uma classificação 31.13% (ID: 259259690_20093.abm)
qui 26. nov 16:21:29 2009 4013 Um dos anexos possui uma URL proibida pelas configurações do Filtro de URL
qui 26. nov 16:21:29 2009 4013 Um dos anexos possui uma URL proibida pelas configurações do Filtro de URL
qui 26. nov 16:21:29 2009 2015 Criado clone de nova mensagem Pol: 6
qui 26. nov 16:21:29 2009 1010 Sucesso ao notificar serviço Engine sobre nova mensagem
qui 26. nov 16:21:29 2009 1013 Mensagem aceita no contexto do serviço Inbound
Marcar como SPAM
Marcar como HAM
Sair

Figura 84. Visualizador de log - eventos.

Filtros do Log de Eventos

Para facilitar a visualização ou procura por algum evento específico, é possível também filtrá-los. Basta clicar sobre o botão **"Filtrar"**, localizado na barra de ferramentas do **Aker Control Center**.

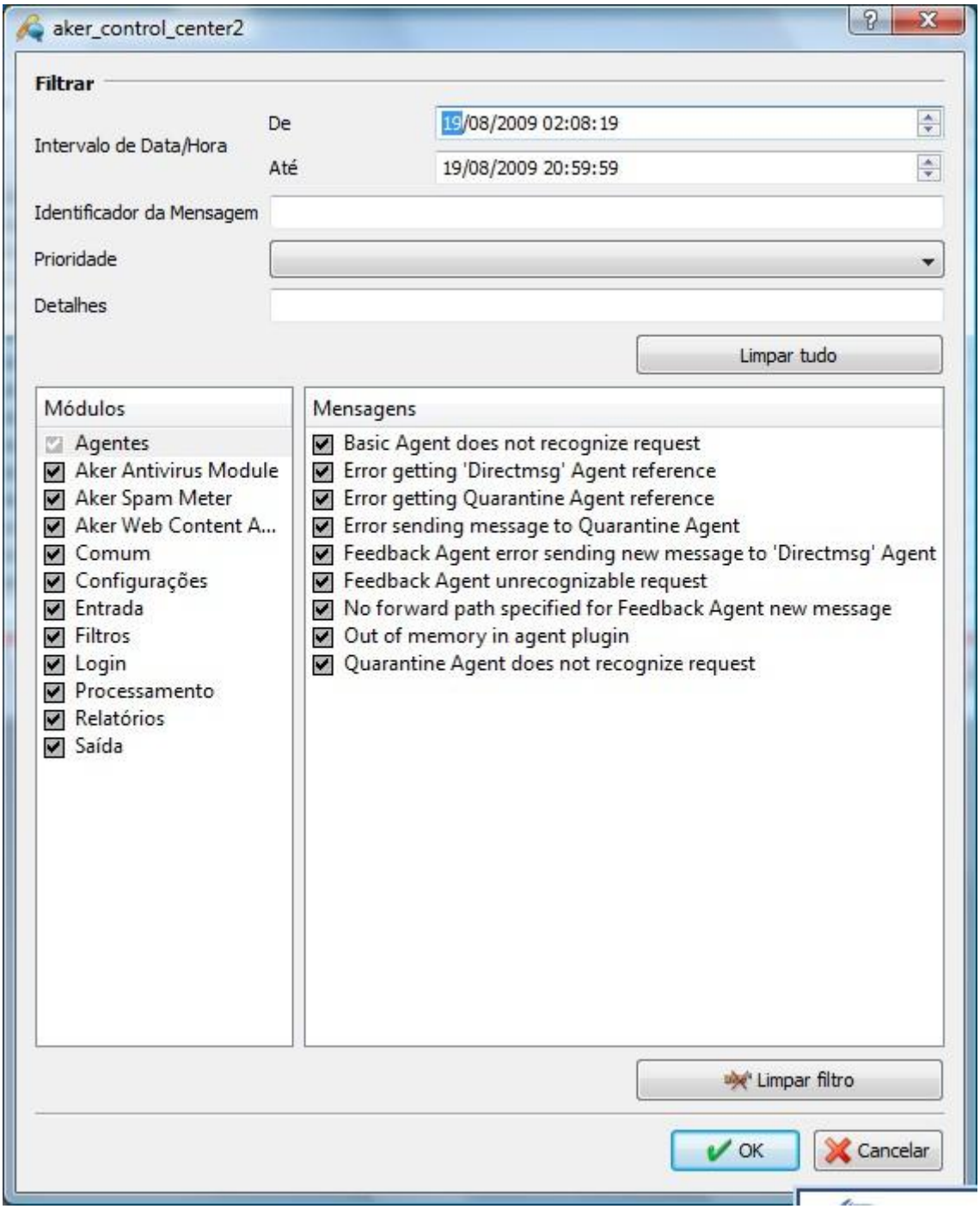

Figura 85. Filtros.

As opções disponíveis para filtragem são:

- Intervalo de data e hora (início e fim);
- Identificador de mensagem relacionada (serve para filtrar os eventos diretamente relacionados ao processamento de uma mensagem específica);
- Prioridade (significado descrito logo acima);
- ID do evento (onde é possível filtrar um evento específico);

- Detalhes (onde é possível filtrar as informações contidas no campo de detalhes).

No caso do filtro de logs diretamente relacionados a uma mensagem, o valor do campo **"Identificador da Mensagem"** pode ser preenchido de duas maneiras:

- Automaticamente, através de duplo clique na mensagem desejada, a partir da aba de log de mensagem (a janela irá mudar automaticamente para a aba de eventos assim que a pesquisa de log for finalizada).
- Manualmente, neste caso obtendo o valor válido do identificador da mensagem através do código fonte da mesma, que é o valor da tag de cabeçalho denominada X-AkerSMTPGW-MessageID.

Tanto no caso do log de mensagem como no do log de eventos, é possível utilizar qualquer combinação de parâmetros para realizar a filtragem.

O ASMG apresenta os logs na ordem inversa em que acontecem (os mais recentes são apresentados nas primeiras telas). Além disso, uma quantidade limitada de logs é mostrada por página. Para visualizar possíveis logs existentes para o filtro atual, é necessário utilizar as opções de **"Próximo"** e **"Anterior"** existentes na barra de ferramentas do Aker Control Center.

É possível visualizar logs a partir de um binário de linha de comando no ASMG. Para tanto, basta utilizar o comando **/usr/local/akmailgw/logviewerif**. Ao invocar o comando sem nenhum parâmetro, será apresentada uma lista completa de opções e sintaxe de uso.

© Aker Security Solutions

Figura 86. Configurações de log – ações das mensagens.

Mensagens para diferentes produtos só irão aparecer em casos de equipamentos de BOX do ASMG que tenham os produtos Aker Spam Meter, Aker Antivírus Module ou Aker Web Content Analyzer integrados.

Plugins

12. Plugins

Esta parte da árvore de configuração apresenta a integração do **ASMG** com outros produtos da Aker para efeito de realização de filtragens de e-mails. Ao integrar-se o ASMG com outras ferramentas, espera-se maior eficiência no controle das mensagens indesejadas, já que abrimos novas opções na procura por arquivos ou mensagens indevidas.

Os produtos Aker os quais possuem integração com o ASMG para efeito de filtragem de e-mails são:

- **Aker Antivírus Module:** produto especializado em filtragem de arquivos em busca de vírus, trojans e outros programas maliciosos;
- **Aker Web Content Analyzer:** produto especializado em classificar URLs em categorias pré-definidas, possibilitando um controle de acesso por estas categorias, quando devidamente integrado a outros produtos Aker;
- **Aker Spam Meter:** produto especializado em realizar a análise bayesiana em mensagens eletrônicas.

Os produtos mencionados são comercializados à parte e o funcionamento do ASMG não está condicionado a qualquer integração com os mesmos. Na ausência deles, apenas as filtragens a que se referem ficarão indisponíveis.

Aker Antivírus Module

Esta janela é utilizada para configurar o acesso ao servidor onde o Aker Antivírus Module está instalado. O Aker Antivírus Module é o programa que efetivamente conhece a base de dados de vírus e é capaz de examinar arquivos a procura deles.

Em relação ao funcionamento, o **ASMG** envia os anexos presentes nas mensagens eletrônicas para esse agente e analisa a resposta. A integração com o ASMG ocorre no sentido de impedir que e-mails com vírus entrem na rede a partir de e-mails.

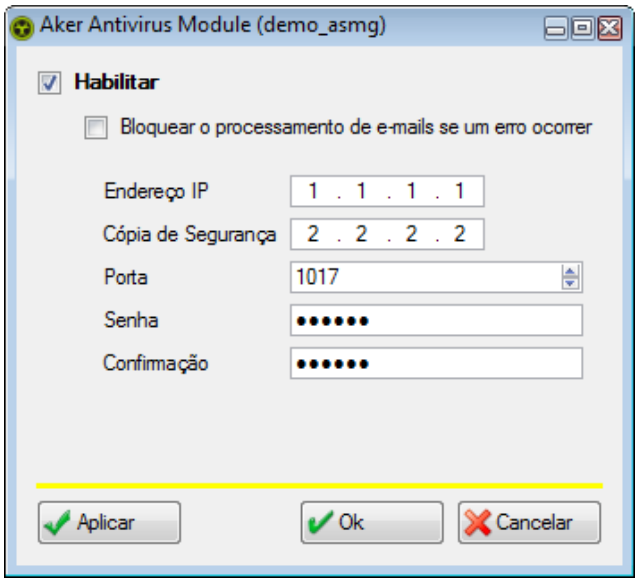

Figura 87. Configuração de acesso ao servidor.

Nesta tela são informados apenas os dados de comunicação entre o servidor Aker Antivírus Module e o **ASMG** e, por isso, só deve ser configurado caso o administrador queira habilitar este tipo de filtragem. Para configurar a comunicação com o Aker Antivírus Module, é necessário informar o endereço IP do servidor onde o agente de antivírus está instalado, o endereço IP de um segundo servidor, para ser acionado em casos de falha do primeiro (caso exista este segundo servidor), o número da porta de comunicação, a senha de segredo compartilhado e sua confirmação.

A porta padrão do serviço oferecido pelo Aker Antivírus Module é a 1017.

Caso você possua uma versão BOX do ASMG, assim como a licença de uso do Aker Antivírus Module, a configuração da comunicação entre os dois produto é um pouco diferente. Nestes casos, a interface gráfica oferecerá a opção de utilização de agente local, a qual deve ser marcada pelo administrador, a fim de que a versão do Aker Antivírus Module utilizada na comunicação seja a local, instalada no equipamento de BOX.

Aker Web Content Analyzer

O Aker Web Content Analyzer é outro produto Aker que pode ter sua funcionalidade agregada ao **ASMG**. Nesta integração, o último envia URLs encontradas em anexos do tipo texto para o primeiro, recebendo a categoria em que se enquadra a URL como resposta e podendo filtrar os anexos com base nestas categorias. A intenção é que, através desta ferramenta, o **ASMG** consiga aumentar a confiabilidade em bloquear mensagens enviadas por spammers, que contenham URLs não permitidas.

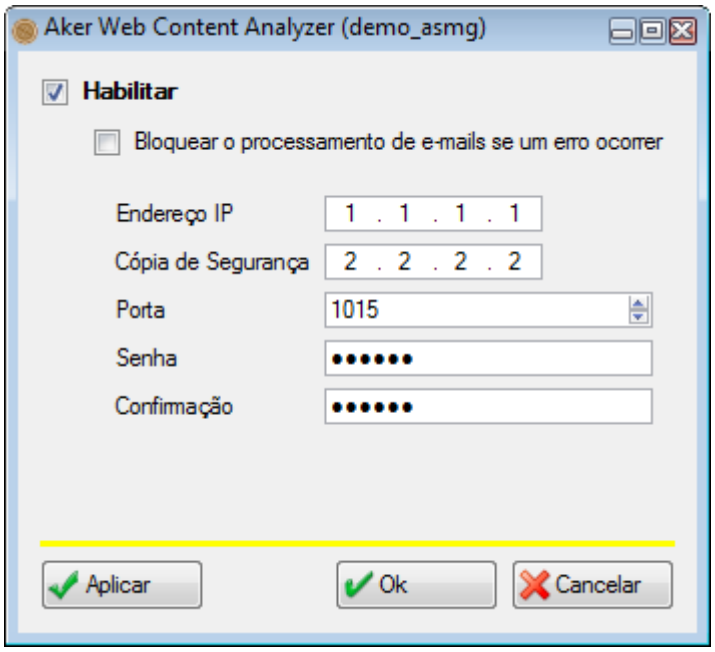

Figura 88. Aker web content analyzer.

A porta padrão do serviço oferecido pelo Aker Web Content Analyzer é a 1015.

Caso você possua uma versão BOX do ASMG, assim como a licença de uso do Aker Web Content Analyzer, a configuração da comunicação entre os dois produto é um pouco diferente. Nestes casos, a interface gráfica oferecerá a opção de utilização de agente local, a qual deve ser marcada pelo administrador, a fim de que a versão do Aker Web Content Analyzer utilizada na comunicação seja a local, instalada no equipamento de BOX.

Aker Spam Meter

A integração do ASMG com este produto oferece à empresa usuária do ASMG uma sofisticada solução de antispam. Baseando-se na técnica de análise bayesiana, o Aker Spam Meter informa ao ASMG a probabilidade de um e-mail ser SPAM. Este último, então, toma uma decisão de filtragem com base na classificação recebida.

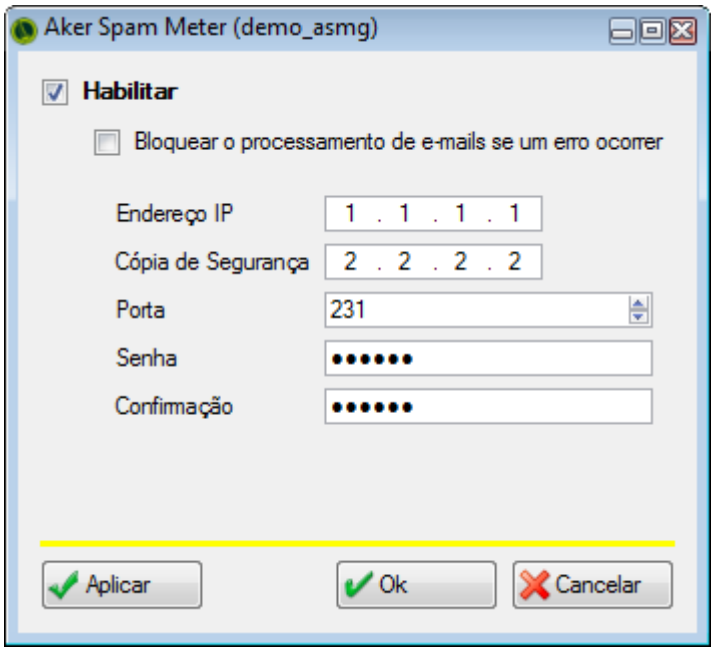

Figura 89. Habilitação do Aker Spam Meter.

A porta padrão do serviço oferecido pelo Aker Spam Meter é a 231.

Caso você possua uma versão BOX do ASMG, assim como a licença de uso do Aker Spam Meter, a configuração da comunicação entre os dois produto é um pouco diferente. Nestes casos, a interface gráfica oferecerá a opção de utilização de agente local, a qual deve ser marcada pelo administrador, a fim de que a versão do Aker Spam Meter utilizada na comunicação seja a local, instalada no equipamento de BOX.

Políticas

13. Políticas

Este item é composto pelas seguintes opções:

- Controle de acesso;
- Política Padrão;
- Novas Políticas criadas.

No contexto do ASMG, uma política pode ser entendida com um conjunto de regras de filtragens que são relacionadas a um conjunto de usuários e/ou grupo. Na prática, as políticas são utilizadas pelo ASMG para permitir que uma mesma mensagem seja filtrada de maneiras distinta pelo ASMG, dependendo do usuário da rede a que ela está relacionada.

Sempre que uma política for criada, um sub-menu correspondente também será criado na árvore de Políticas, com duas sub-árvores: uma para filtrar as mensagens de entrada, e a outra, para as mensagens de saída (também se aplica à Política Padrão). As janelas para estas filtragens são praticamente as mesmas, diferenciando-se as opções que forem referentes a destinatários e remetentes.

Esta subseção irá abordar todos os detalhes sobre criação de políticas, como relacioná-las aos usuários da rede e sobre filtragens disponíveis para serem utilizadas de maneira seletiva em políticas.

Controle de Acesso

Esta janela é a responsável por permitir o gerenciamento de políticas no ASMG. Nela define-se os parâmetros desejados para a Política Padrão, além da criação de outras políticas e associação aos usuários a que elas se referem.

Sempre que criar uma nova política, o administrador deve definir os usuários e grupos aos quais deseja associá-la. Os usuários que não forem referenciados em qualquer política terão suas mensagens analisadas pelo conjunto de regras da "**Política Padrão"**. Esta política é sempre existente.

© Aker Security Solutions

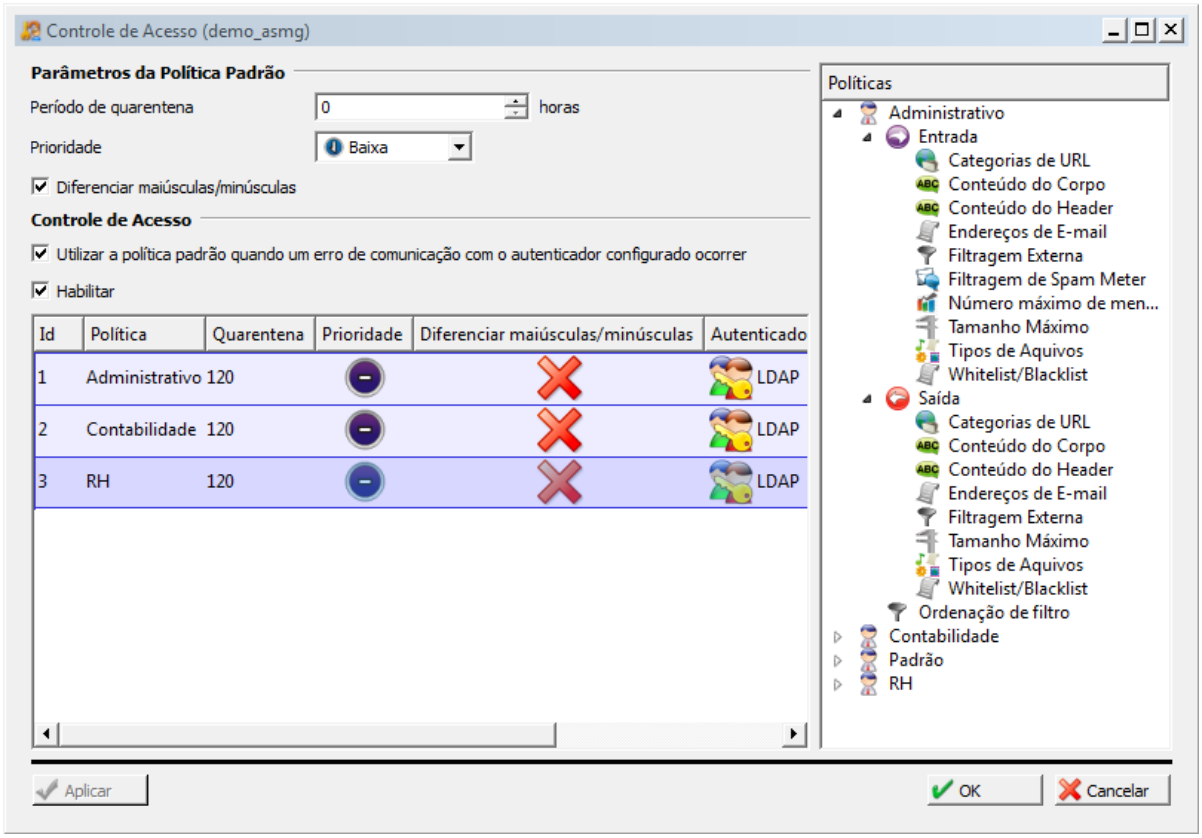

Figura 90. Controle de acesso.

Parâmetros de Configuração para Políticas

As políticas do ASMG possuem alguns parâmetros que precisam ser definidos na configuração. Alguns parâmetros devem ser definidos tanto para a política padrão quanto para as políticas criadas pelo administrador. São eles:

- **Tempo de Quarentena:**

  A quarentena é um repositório de sistema bastante utilizado por basicamente todos os filtros no **ASMG** como opção de ação quando o sistema detecta uma situação de interesse (exemplo: uma mensagem com vírus). O produto oferece a opção de definir um tempo de quarentena distinto para cada política criada.

- **Prioridade:**

  O parâmetro de prioridade é aplicado nas situações em que ocorre enfileiramento das mensagens, devido a um grande volume de processamento. Neste caso as mensagens são enfileiradas e processadas de acordo com a prioridade que foi estabelecida à Política, que pode ser: Muito Baixa, Baixa, Normal, Alta e Muito Alta. Como os nomes sugerem, quanto maior for à prioridade, mais rapidamente a mensagem será processada em situações de grande volume de mensagens pendentes e consequente enfileiramento.

- **Diferenciar Maiúsculas/Minúsculas:**

Este parâmetro é utilizado quando a base de usuários que o ASMG se integra, através do Autenticador é case-sensitive, ou seja, suas bases de usuários ou seus endereços de e-mail são diferenciados com letras maiúsculas e minúsculas.

Criação de Novas Políticas

A criação de novas políticas é realizada a partir de um clique com o botão direito sobre o objeto de lista de políticas, localizado na seção de controle de acesso da janela. Para tanto, o administrador necessita antes informar ao sistema que ele pretende utilizar o controle de acesso, a fim de que o ASMG se prepare para realizar a diferenciação de filtragem nas mensagens com base em seus remetentes/destinatários. Para habilitar o controle de acesso, basta clicar no controle **"Habilitar",** a primeira opção abaixo da seção dedicada às configurações do controle de acesso.

Para criar com sucesso uma nova política, além dos parâmetros de tempo de quarentena e prioridade, é preciso definir alguns outros parâmetros:

Política

Define um nome para a política, que também será o nome que aparecerá na árvore de políticas assim que finalizada a criação da mesma. Sugere-se nomear políticas com uma sequência de caracteres que seja de fácil associação com os usuários que irão participar dela ou com a função que irão desempenhar.

Autenticador

O parâmetro de autenticador, o qual deve ser configurado a partir das entidades de mesmo nome, dentre os que estiverem disponíveis no sistema, associa os usuários e grupos a uma política. Além disso, ele também determina o domínio que deve ser associado à política em questão. Esta associação, não explícita nesta janela, é feita quando da criação da entidade do tipo **"Autenticador"**: neste momento, o usuário necessita cadastrar um ou mais domínios que estarão associados ao autenticador.

Usuários e Grupos

Os usuários e grupos são talvez os parâmetros mais importantes para a criação de uma política. Eles definem à quais usuários e grupos a política criada será associada, ou seja, desvia a filtragem de mensagens relacionadas a estes usuários e grupos para o conjunto de regras de filtragem definidas.

Ao clicar com o botão direito sobre estes campos, o administrador poderá adicionar usuários e grupos com base no autenticador definido pelo parâmetro anterior, ou seja, serão listados todos os usuários e grupos conhecidos pelo autenticador em questão, de modo que se possa escolher qualquer um deles para fazer parte da política. Além disso, é possível que se digite um nome de um usuário ou de um

© Aker Security Solutions

grupo, mesmo que ele não seja conhecido pelo autenticador. Esta opção é útil para a associação de aliases a uma política.

No mecanismo de associação de usuários a políticas, é importante destacar que os usuários da rede são os remetentes, no caso de mensagens enviadas por algum usuário da rede; e são os destinatários, no caso de mensagens enviadas por alguém de fora da rede com destino a um ou mais usuários da rede.

Finalizando a Criação ou Edição de uma Política

Após definir todos os parâmetros necessários, o administrador deverá clicar no botão **"Aplicar"** ou **"Ok"** da janela, a fim de que as novas configurações sejam efetivas. No caso de novas políticas, uma nova subárvore, com o mesmo nome definido para a política criada, será adicionada à subárvore de políticas.

Erros de Comunicação com o Autenticador Relacionado à Política

Autenticadores são programas executados potencialmente em máquinas remotas. Além disso, como todo programa, estão sujeitos a falhas. Em casos de erro de comunicação com o autenticador definido para a política durante o processamento de mensagens, o ASMG permite a adoção de dois possíveis comportamentos:

- As mensagens em processamento podem ser associadas à política padrão. Neste caso, para as mensagens processadas durante o período de indisponibilidade do autenticador, valerão as regras de filtragem da política padrão, não importando quais são os remetentes ou destinatários das mesmas.
- As mensagens em processamento ficam retidas, aguardando o retorno da comunicação com o autenticador. **Além disso, para esta opção, o sistema suspende o recebimento de novas mensagens até o perfeito restabelecimento da comunicação com o autenticador**.

O administrador escolhe um desses comportamentos através da opção **"Utilizar política padrão quando um erro de comunicação com o autenticador configurado ocorrer"**. Se ela estiver marcada, valerá o primeiro comportamento explicado. Caso contrário, valerá o segundo.

Categorias de URL

Esta análise é feita através da integração do **ASMG** com outro produto da Aker: o **Aker Web Content Analyzer (AWCA)**.

É importante destacar que, para a utilização desta filtragem, é indispensável à existência de uma versão do AWCA disponível para comunicação com o ASMG. Se você possui uma versão BOX do ASMG, vai precisar apenas da licença do AWCA. A configuração dos parâmetros de comunicação entre os produtos, também

indispensável para o funcionamento do filtro e que deve ser realizada antes do uso desta janela de filtragem, é explicada em detalhes no capítulo **Plugins**.

O **AWCA** é alimentado com uma grande de base de dados de URLs, subdividida em diversas categorias como: Jogos de Azar, Chat, Nudismo, Esportes, etc. Esta base é alimentada constantemente por uma equipe especializada em categorizar URL's e assim disponibilizar bases atualizadas para os clientes. A idéia principal é que o acesso a certas categorias seja impedido.

Após a verificação de que há uma URL no anexo da mensagem, o **ASMG** a encaminha para o Analisador. Caso alguma delas coincida com uma URL bloqueada, há as opções de remover o anexo ou descartar a mensagem. Caso ocorra a remoção do anexo apenas, uma mensagem de notificação será adicionada à mensagem original, informando que ele foi removido. Como opções adicionais, o administrador pode encaminhar uma cópia da mensagem para a quarentena, encaminhá-la para algum endereço de e-mail e/ou considerar as URL's que não estiverem no banco de dados como **"indefinida".**

Entrada

Nesta tela, configuram-se as categorias de URLs que podem bloquear/permitir nos anexos das mensagens que chegam aos usuários internos do **ASMG**. Não há restrições quanto ao número de URLs selecionadas.

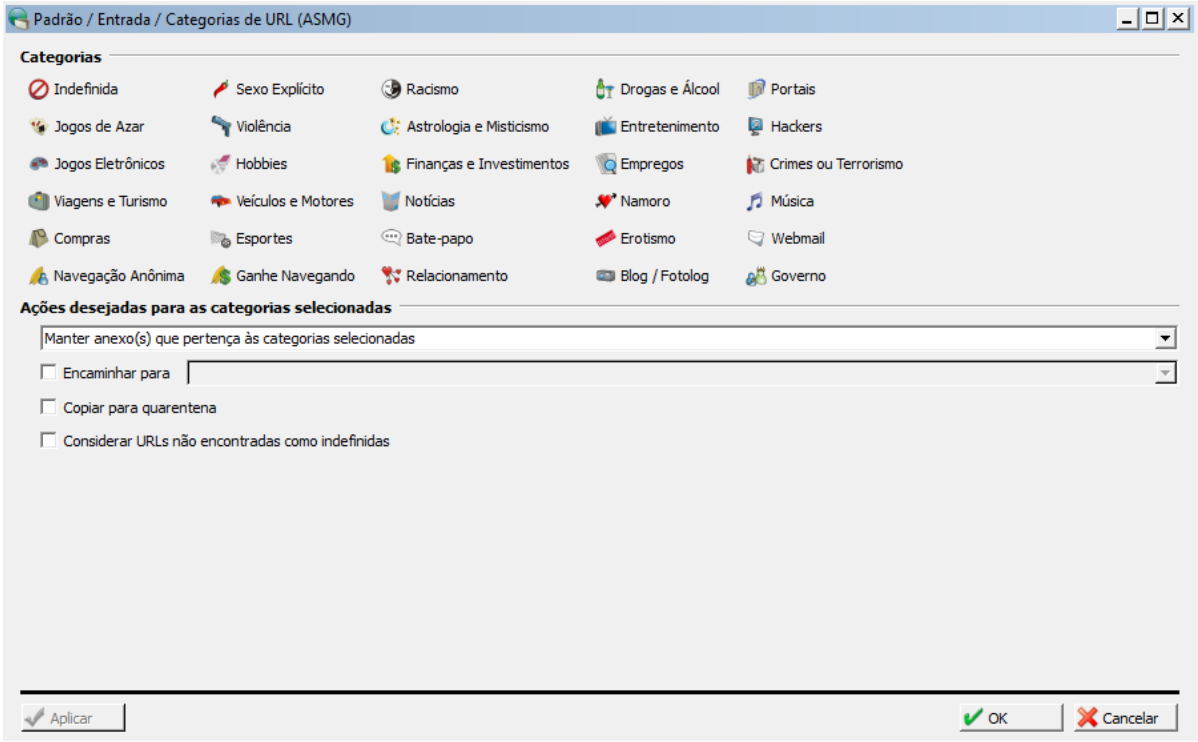

Figura 91. Categorias de URL's – entradas.

Saída

Nesta tela configuram-se as categorias de URLs que podem bloquear/permitir nos anexos das mensagens que são enviadas aos destinatários externos do **ASMG**. Não há restrições quanto ao número de URLs selecionadas.

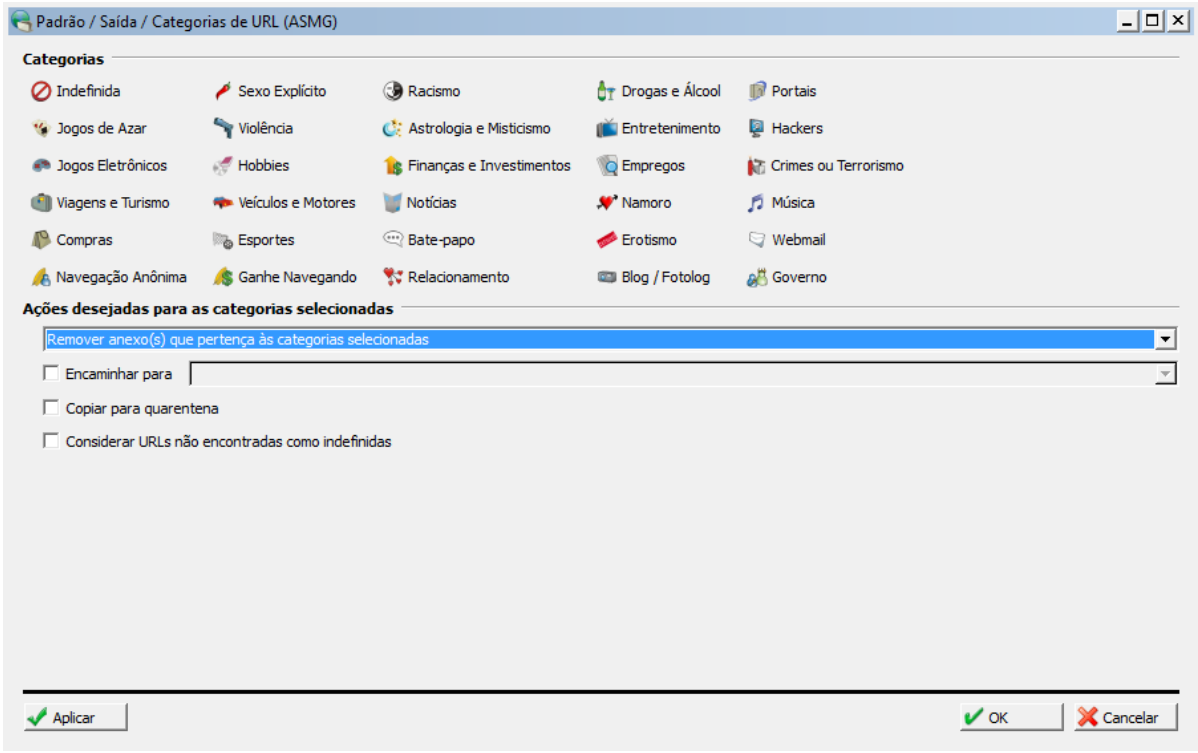

Figura 92. Configuração das categorias de URL's – saída.

Nas duas janelas, ao habilitar a opção **"Considerar URL's não encontradas como indefinidas",** aparecerá uma janela de confirmação na qual informará os riscos que esta opção pode gerar como mostra a imagem abaixo:

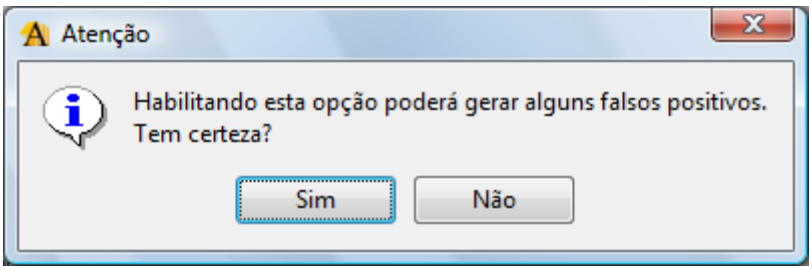

Figura 93. Janela de confirmação sobre geração de falsos positivos.

Clicar no botão "**SIM"**, significa permitir que as URL's não encontradas na base de dados sejam consideradas como pertencentes à categoria **"Indefinida"**. Caso contrário a opção será desmarcada automaticamente.

Esta configuração pode gerar alguns *FALSOS POSITIVOS*, ou seja, qualquer texto que se pareça com uma URL no anexo da mensagem poderá bloqueá-la.

Conteúdo do Corpo e Conteúdo do Header

13..1. Conteúdo do Corpo

Nestas janelas configuram-se restrições para palavras-chave/expressões regulares contidas em anexos do tipo texto das mensagens enviadas ou recebidas pelos usuários internos. As janelas de **“Entrada”** e **“Saída”** possuem as abas **"Palavras-Chave"** e **"Expressões Regulares"**.

Na aba **"Palavras-chave"** podem-se inserir listas de palavras previamente cadastradas em entidades do tipo **"Lista de Palavras-Chave"**. As operações possíveis de serem realizadas são: remover anexos de mensagens que se encaixem no padrão encontrado ou manter anexos. Neste caso, uma mensagem de notificação será colocada junto à mensagem original, informando ao destinatário que ali havia um anexo e que este foi removido. Além disso, é possível encaminhar a mensagem para algum e-mail interno ou copia-lá para quarentena.

Já na aba **"Expressões Regulares"** podem-se inserir listas de expressões previamente cadastradas em entidades do tipo **"Listas de Expressão Regular"**, que definem um padrão de palavras. Com elas é possível identificar facilmente, por exemplo, se existe um anexo que faça referência a algum endereço eletrônico, ou URL qualquer. As operações possíveis de serem realizadas são: remover anexos de mensagens que se encaixem no padrão mencionado ou pular para o próximo filtro. Neste caso, uma mensagem de notificação será colocada junto à mensagem original, informando ao destinatário que ali havia um anexo e que este foi removido. Além disso, é possível encaminhar a mensagem para algum e-mail interno ou copia-la para a quarentena.

Entrada

Nesta aba configuram-se as listas de expressões regulares e palavras-chave que serão analisadas em mensagens que chegam para os usuários internos (destinatários).

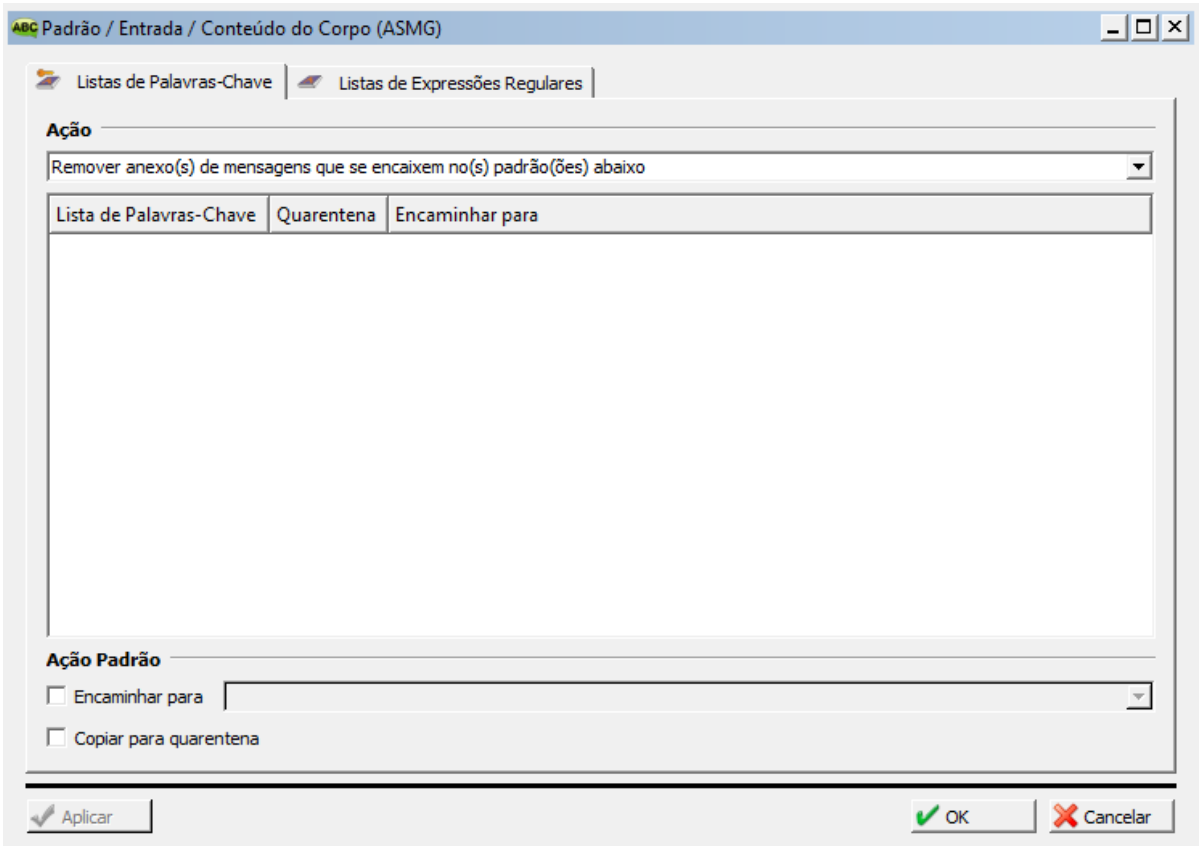

Figura 94. Conteúdo do corpo – lista de palavras chaves.

Nesta tela, o administrador opta por fazer pesquisas no corpo da mensagem, de determinadas palavras previamente cadastradas em uma lista do tipo **"Listas de palavras-chave"**. Segue o procedimento para realizar esta configuração:

- Clicar com o botão direito do mouse em qualquer lugar do quadro e escolha a opção "Inserir";
- Em seguida, clicar com o botão direito do mouse sob a coluna **"Lista de Palavras-Chave"** e escolher a opção **"Adicionar Entidades"**;
- Selecione a entidade do tipo **"Lista de Palavras-Chave"** que deseja adicionar à regra. Clique em **"Adicionar"**;
- Para indicar se a mensagem deve ir para a quarentena ou não, clicar com o botão direito do mouse sob a coluna **"Quarentena"** e escolher entre as opções **"Habilitar"** ou **"Desabilitar"**;
- Se desejar encaminhar uma cópia da mensagem para alguém, deve-se clicar com o botão direito do mouse sob a coluna **"Encaminhar para"**, selecionar a opção **"Adicionar Entidades"** e escolher a entidade do tipo **"Lista de E-mail"** desejada. Clicar em **"Adicionar"**.

Saída

Nestas abas configuram-se expressões regulares e palavras-chave que serão analisadas em mensagens enviadas pelos usuários internos (remetentes).

13..2. Conteúdo do Header

Nestas janelas configuram-se restrições para palavras-chave/expressões regulares contidas no Header das mensagens enviadas ou recebidas pelos usuários internos. As janelas de Entrada e Saída possuem as abas **"Palavras-Chave"** e **"Expressões Regulares"**.

Na aba **"Palavras-chave"** podem-se inserir listas de palavras previamente cadastradas em entidades do tipo **"Lista de Palavras-Chave".** As operações possíveis de serem realizadas são: pular para o próximo filtro mensagens que se encaixem no padrão mencionado ou descartá-las. Além disso, é possível encaminhar a mensagem para algum e-mail interno ou copia-lá para a quarentena.

Já a aba **"Expressões Regulares"** permite inserir listas de expressões previamente cadastradas em entidades do tipo **"Listas de Expressão Regular"**, que definem um padrão de palavras. Com elas é possível identificar facilmente, por exemplo, se existe no Header algum endereço eletrônico, ou URL qualquer. As operações possíveis de serem realizadas são: pular para o próximo filtro as mensagens que se encaixem no padrão mencionado ou descartá-las. Além disso, é possível encaminhar a mensagem para algum e-mail interno ou movê-la para quarentena.

Entrada

Nestas abas configuram-se as listas de expressões regulares e palavras-chave que serão analisadas em mensagens que chegam para os usuários internos (destinatários).

Esta tela tem a opção por fazer pesquisas de determinadas palavras previamente cadastradas em uma lista do tipo **"Listas de palavras-chave".** Para realizar esta configuração, basta seguir o procedimento abaixo:

- Clicar com o botão direito do mouse em qualquer lugar do quadro e escolha a opção "Inserir";
- Em seguida, clicar com o botão direito do mouse sob a coluna **"Lista de Palavras-Chave"** e escolher a opção **"Adicionar Entidades"**;
- Selecionar a entidade do tipo **"Lista de Palavras-Chave"** que deseja adicionar à regra. Clicar em **"Adicionar"**;
- Para indicar se a mensagem deve ir para a quarentena ou não, deve-se clicar com o botão direito do mouse sob a coluna **"Quarentena"** e escolher entre as opções **"Habilitar"** ou **"Desabilitar"**;
- Se desejar encaminhar uma cópia da mensagem para alguém, deve-se clicar com o botão direito do mouse sob a coluna **"Encaminhar para"**, selecionar a opção **"Adicionar Entidades"** e escolher a entidade do tipo **"Lista de E-mail"** desejada. Clicar em **"Adicionar"**.

© Aker Security Solutions

Saída

Nestas abas configuram-se expressões regulares e palavras-chave que serão analisadas em mensagens enviadas pelos usuários internos (remetentes).

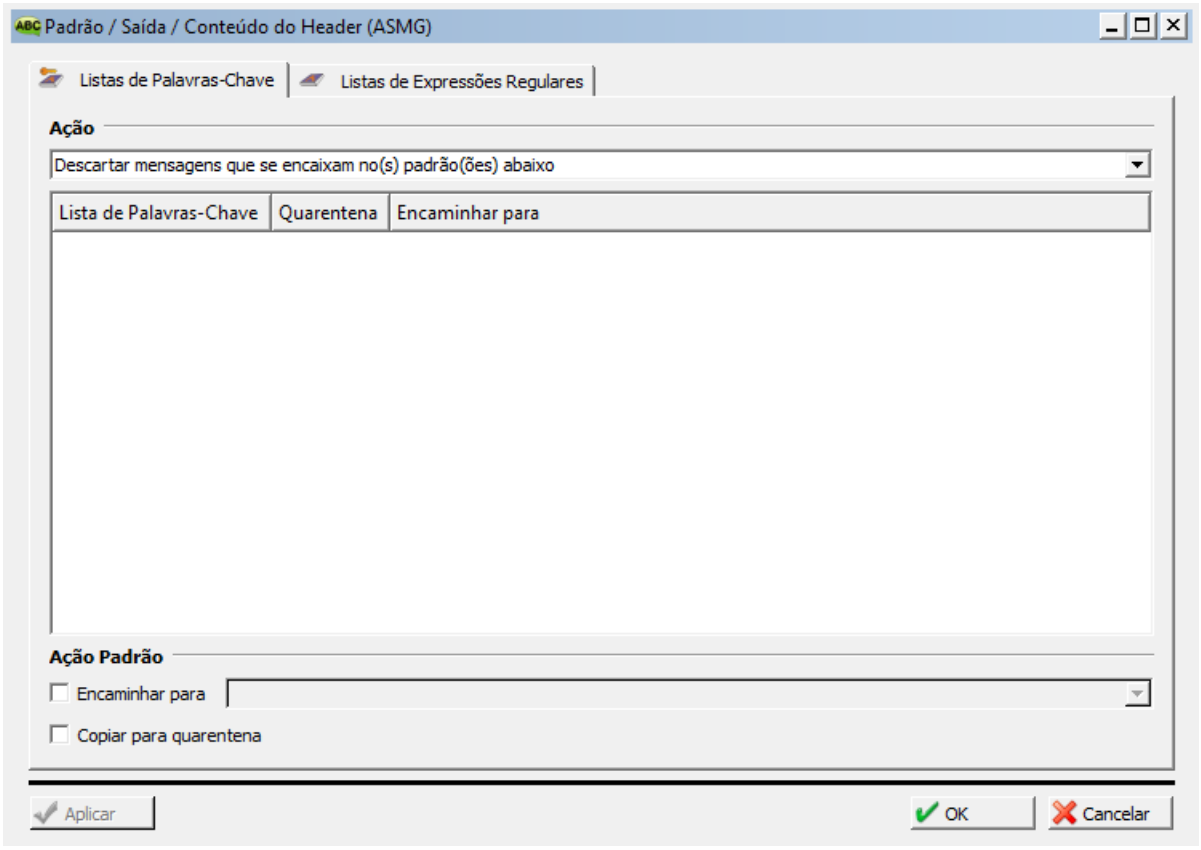

Figura 95. Conteúdo do header – lista de palavras chaves.

Endereços de Email

Este filtro é especializado em restringir os remetentes dos quais os usuários associados à política em questão estão autorizados a receber mensagens e também para quais destinatários estes usuários podem enviar mensagens. A filtragem ocorre, portanto, no parâmetro de remetente da mensagem, quando enviadas de fora da rede; e nos destinatários, quando enviados de dentro da rede. Na chegada de mensagens o **ASMG** trata os usuários internos como destinatários e os externos como remetentes. A posição se inverte quando a mensagem é enviada por um cliente interno.

Para essa filtragem, é permitido ao administrador definir se deseja pular para o próximo filtro ou descartar as mensagens que não coincidam com os padrões

mencionados, se deseja encaminhá-las para algum endereço de e-mail e/ou se elas devem ser enviadas para a quarentena.

Entrada

Na aba **"Domínios dos Remetentes"** define-se as restrições aos domínios dos remetentes (os que podem e os que não podem enviar mensagens aos destinatários).

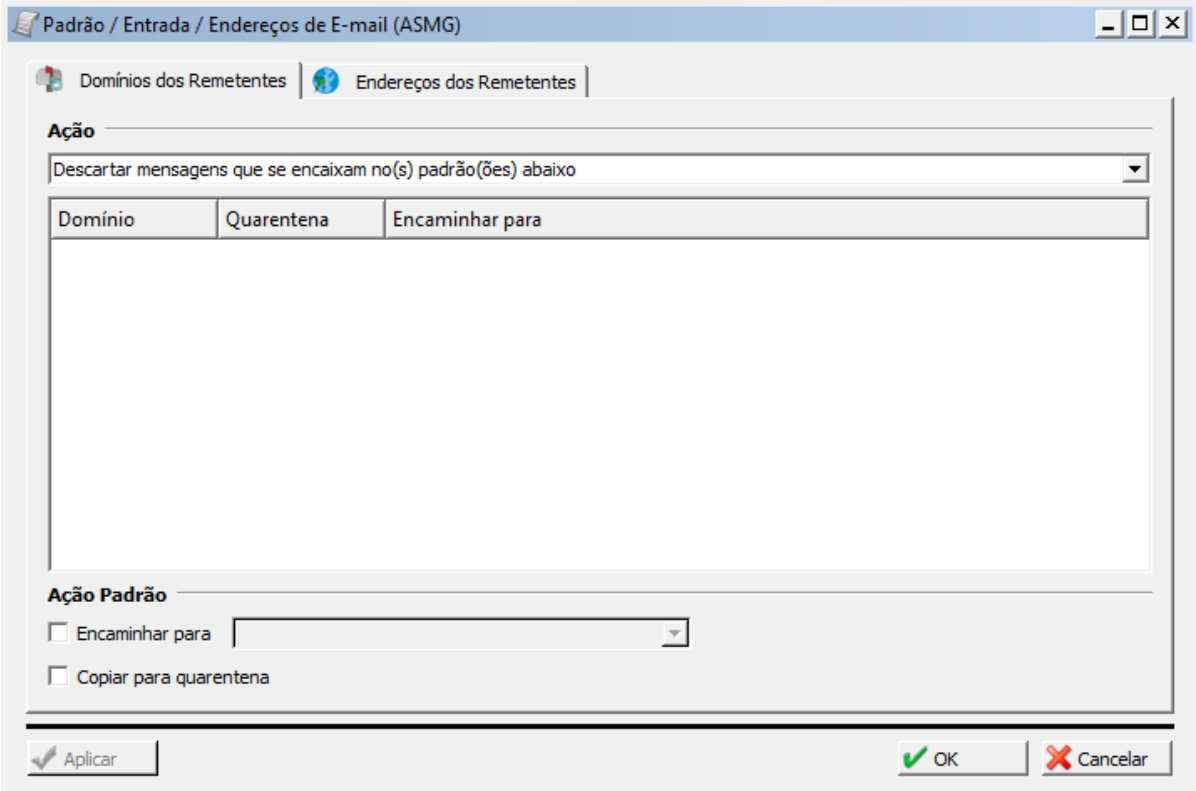

Figura 96. Endereços de e-mail – descarte de mensagens nos padrões descritos.

Ação – Descartar mensagens que se encaixam no(s) padrão(ões) abaixo: Se esta opção estiver selecionada, todos os e-mails vindos dos domínios listados na janela serão passados para o próximo filtro e os outros e-mails que não se encaixarem serão bloqueados.

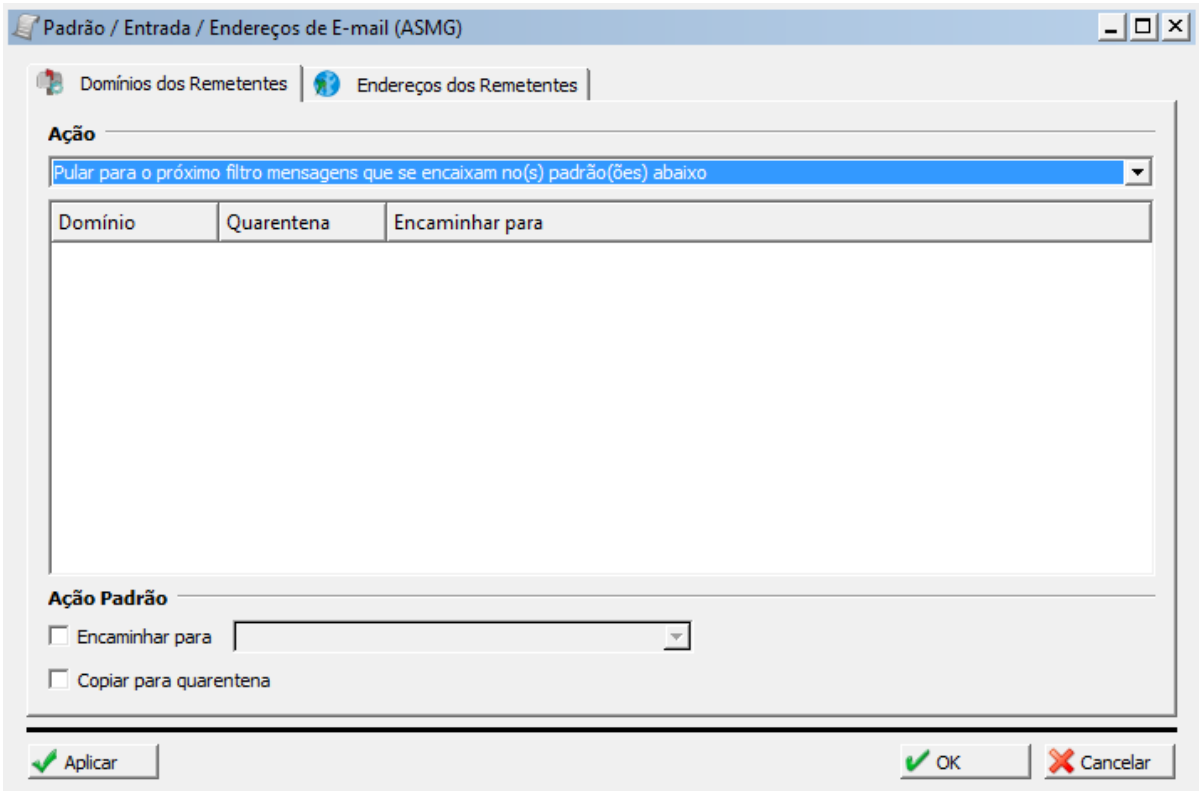

Figura 97. Endereços de e-mail – pular para o próximo filtro mensagens que se encaixam no padrão.

Ação – Pular o próximo filtro mensagens que se encaixam no(s) padrão(ões) abaixo: Se esta opção estiver selecionada, todos os e-mails, cujos remetentes dos domínios listados na janela serão bloqueados e os outros e-mails que não se encaixarem serão passados para o próximo filtro.

O exemplo abaixo mostra o bloqueio do domínio *blockdomain.com* quanto ao envio de mensagens para os usuários internos. A configuração dos dados deve ser da seguinte maneira:

- Clicar com o botão direito do mouse em qualquer lugar do quadro e escolher a opção **"Inserir";**
- Em seguida, clicar com o botão direito do mouse sob a coluna **"Domínio"** e escolher a opção **"Adicionar Entidades";**
- Selecionar a entidade do tipo **"Domínio"** que deseja que seja adicionada à regra. Clicar em **"Adicionar"**;
- Para indicar se a mensagem deve ir para a quarentena ou não, deve-se clicar com o botão direito do mouse sob a coluna **"Quarentena"** e escolher entre as opções **"Habilitar"** ou **"Desabilitar"**;
- Se desejar encaminhar uma cópia da mensagem para alguém, clique com o botão direito do mouse sob a coluna **"Encaminhar para"**, selecione a opção **"Adicionar Entidades"** e escolha a entidade do tipo **"Lista de E-mail"** desejada. Clicar em **"Adicionar"**.

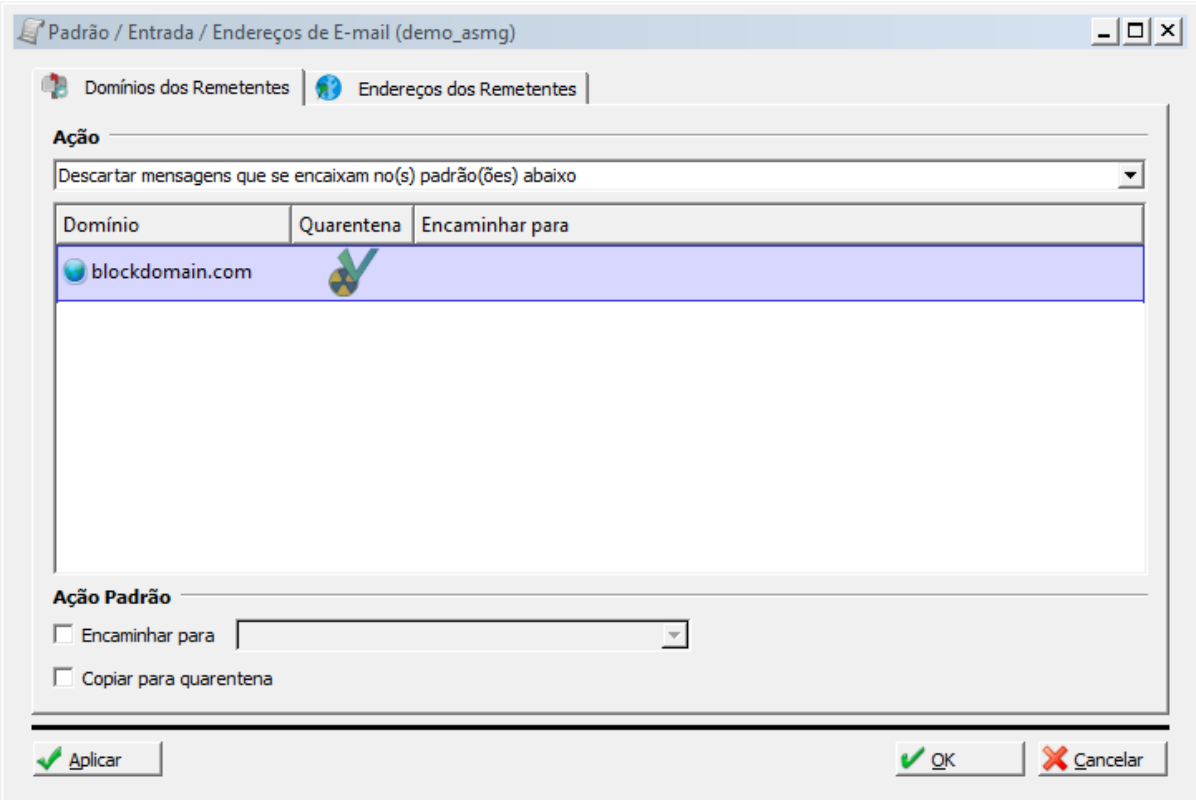

Figura 98. Endereços de e-mail – domínio dos rementes.

Na aba **"Endereços dos Remetentes"** pode-se definir restrições aos endereços dos remetentes (os que podem e os que não podem enviar mensagens aos destinatários).

Ação - Descartar mensagens que se encaixam no (s) padrão(ões) abaixo: Se esta opção estiver selecionada, todos os remetentes listados na janela serão passados para o próximo filtro e os outros e-mails que não se encaixarem serão bloqueados.

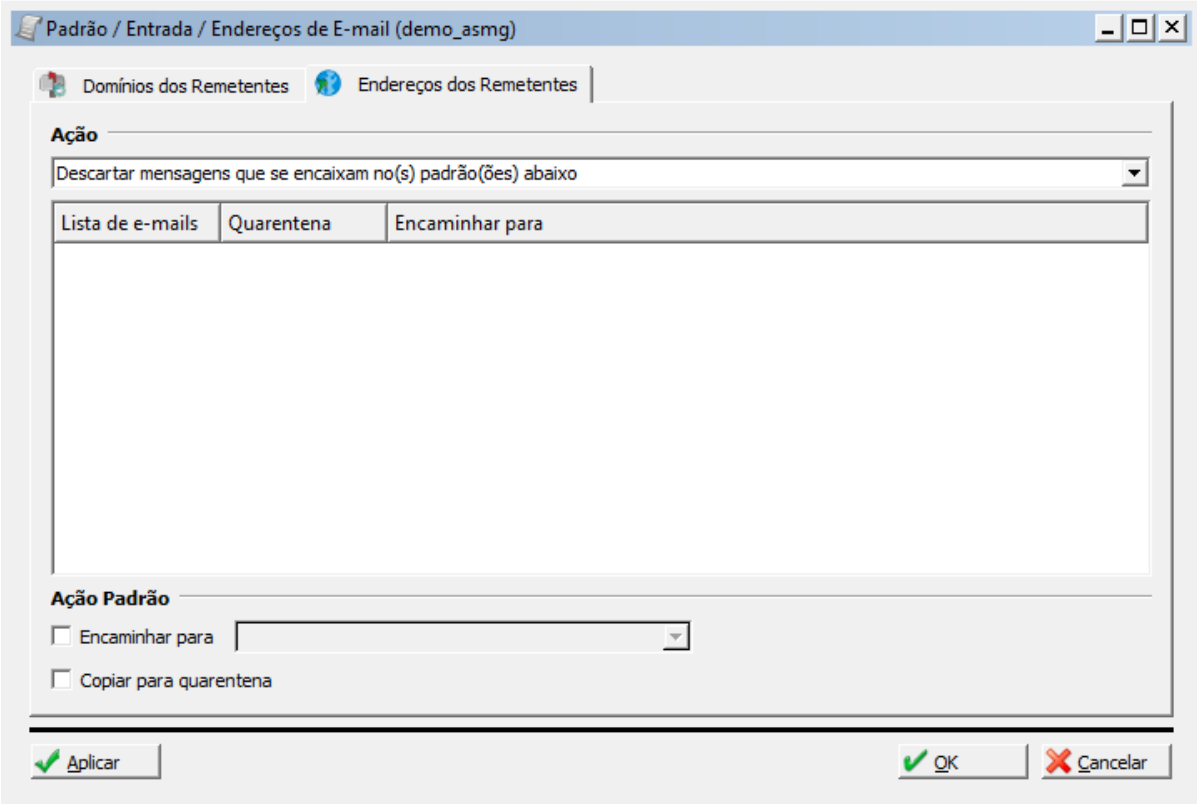

Figura 99. Endereços de e-mail – endereço dos remetentes.

Ação – Pular o próximo filtro mensagens que se encaixam no(s) padrão(ões) abaixo: Se esta opção estiver selecionada, todos os remetentes listados na janela serão bloqueados e os outros e-mails que não se encaixarem serão passados para o próximo filtro.

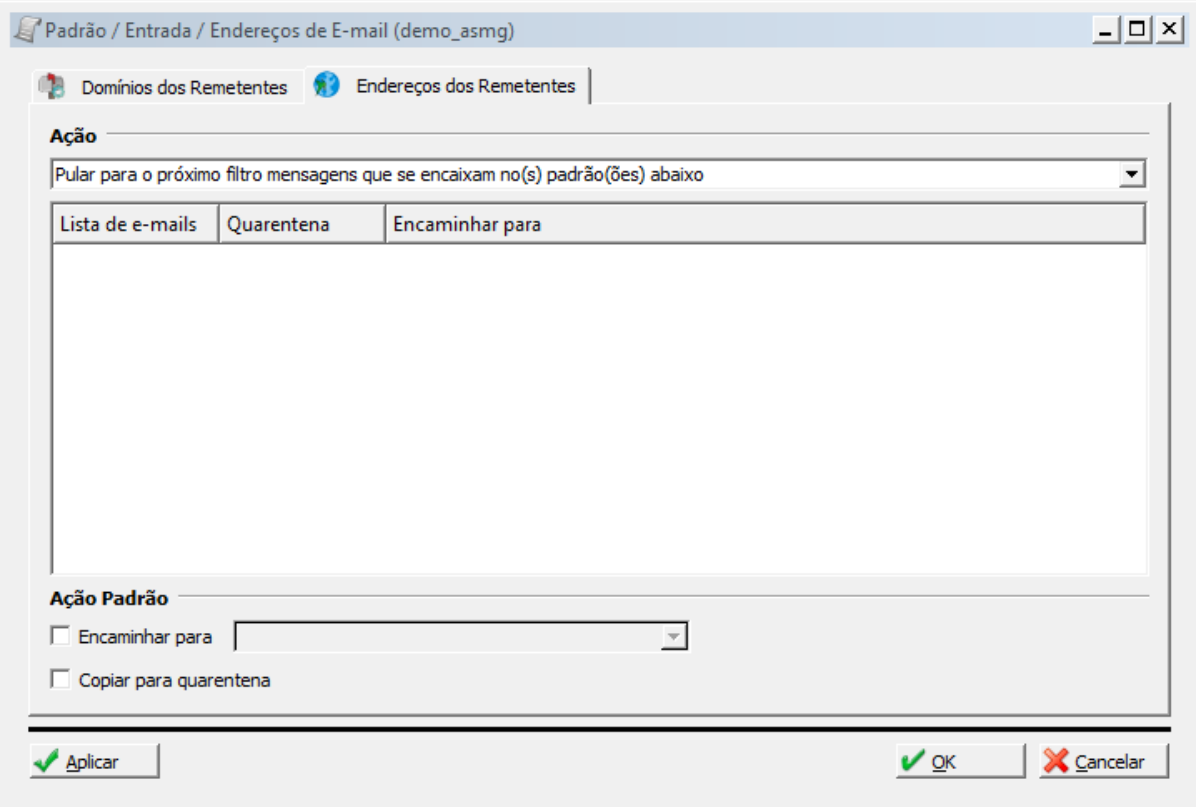

Figura 100. Endereços de e-mail – endereço dos remetentes (pular para o próximo filtro).

Saída

Na aba **"Domínios dos Destinatários"** pode-se definir os domínios dos destinatários para quem os usuários internos podem enviar ou não suas mensagens.

Já na aba **"Endereços dos Destinatários"** pode-se definir os endereços daqueles destinatários para quem os usuários internos não possuem permissão para envio de mensagens. Por padrão, os endereços que não estiverem listados neste quadro terão as mensagens repassadas normalmente.

Para configurar dados em ambas as janelas, basta seguir os mesmos passos para a configuração de **"Domínios dos Remetentes"**, apenas lembrando que o envio agora acontece dos usuários internos para a Internet.

Filtragem Externa

Através da integração com filtros e scripts externos, cadastrados previamente como entidades do tipo **"Filtro Externo",** o **ASMG** aumenta sua capacidade de filtragem de mensagens indevidas.

O processo se dá com o envio da mensagem pelo **ASMG** para estes programas, normalmente antivírus ou analisadores de SPAM, e, com base na resposta dos mesmos, a mensagem pode ser descartada ou enviada com o campo de assunto modificado para os destinatários. Cada programa/script externo deve ser configurado como uma entidade antes de ser utilizado nesta janela.

É necessário reiterar que o **ASMG** apenas envia a mensagem para o programa especificado, mas a configuração e comportamento deste último devem ser feitos de maneira completamente independente para que os resultados esperados possam ser atingidos.

Entrada

Nesta tela configuram-se as ações que podem ser executadas pelos filtros externos em relação às mensagens recebidas pelos usuários internos (destinatários).

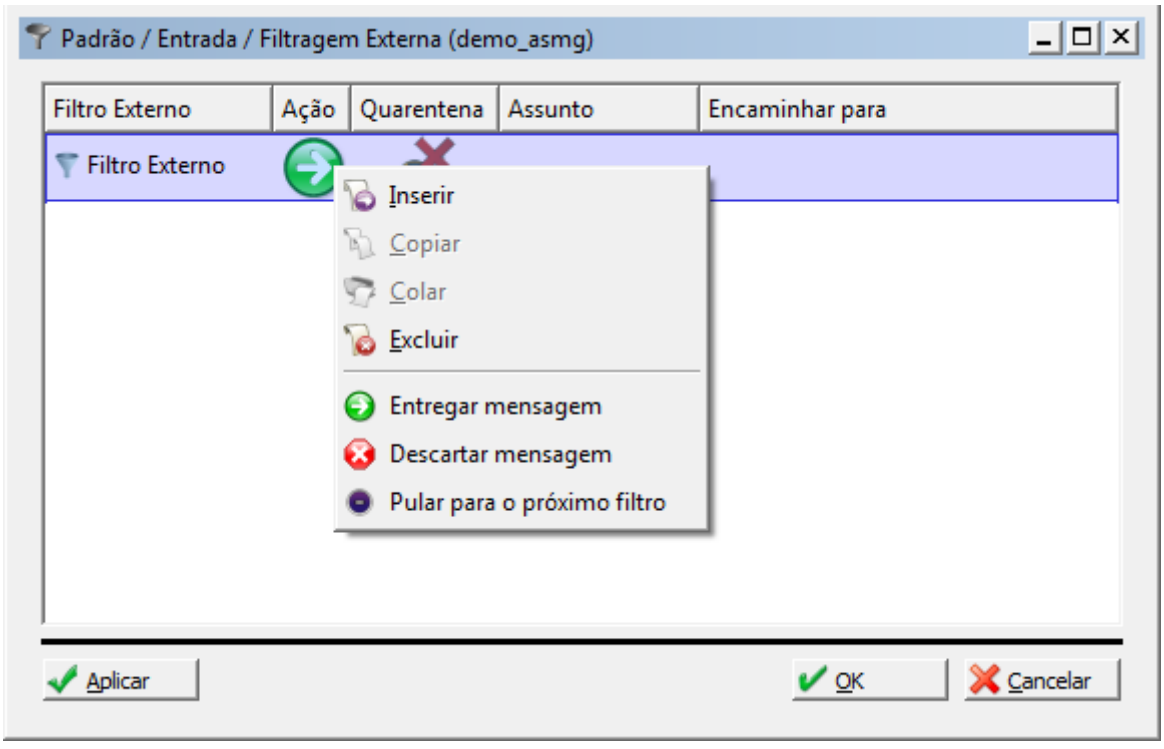

Figura 101. Filtragem externar – ações que podem ser executadas pelos filtros externos.

Para realizar esta configuração:

- Clicar com o botão direito do mouse em qualquer lugar do quadro e escolha a opção "Inserir";

- Em seguida, clicar com o botão direito do mouse sob a coluna **"Filtro Externo"** e escolher a opção **"Adicionar Entidades"**;
- Selecionar a entidade do tipo **"Filtro Externo"** que deseja adicionar à regra. Clicar em **"Adicionar"**;
- Em seguida, defina o tipo de ação a ser tomada. Para isso, clique com o botão direito do mouse sob a coluna **"Ação"** e escolha entre as opções **"Aceitar Mensagem"** ou **"Descartar Mensagem"**;
- Para indicar se a mensagem deve ir para a quarentena ou não, deve-se clicar com o botão direito do mouse sob a coluna **"Quarentena"** e escolher entre as opções **"Habilitar"** ou **"Desabilitar"**;
- Se desejar encaminhar uma cópia da mensagem para alguém, deve-se clicar com o botão direito do mouse sob a coluna **"Encaminhar para"**, e selecionar a opção **"Adicionar Entidades"** e escolher a entidade do tipo **"Lista de E-mail"** desejada. Clicar em **"Adicionar"**.

Saída

Nesta tela configuram-se as ações que podem ser executadas pelos filtros externos em relação às mensagens enviadas pelos usuários internos (remetentes).

Exemplo: Definiu-se que todas as mensagens que saem da área controlada pelo **ASMG** devem ser examinadas. Conforme foi definido na configuração da Entidade do tipo "Filtro Externo", sempre que ocorrer um comportamento que sugira que a mensagens está infectada, o antivírus retorna um código ao **ASMG**, indicando o problema. Neste caso, estamos indicando que a mensagem seja descartada e uma cópia dela seja encaminhada para o Administrador, para que seja feita a análise necessária.

Filtragem de Spam Meter

A filtragem de Spam Meter utiliza a integração do ASMG com o Aker Spam Meter (ASM), um produto especializado em realizar análise bayesiana sobre mensagens eletrônica. Esta filtragem utiliza técnicas de armazenamento das características das mensagens, numa operação denominada de treinamento, com a associação destas características a contextos de SPAM e não SPAM, gerando bases de dados com estes dois perfis. A partir das informações armazenadas nestas bases, são empregadas técnicas matemáticas em novas mensagens recebidas para que ao final exista a definição da probabilidade de elas serem SPAM.

É importante destacar que, para a utilização desta filtragem, é indispensável a existência de uma versão do ASM disponível para comunicação com o ASMG. Se você possui uma versão BOX do ASMG, vai precisar apenas da licença do ASM. A configuração dos parâmetros de comunicação entre os produtos, também indispensável para o funcionamento do filtro e que deve ser realizada antes do uso desta janela de filtragem, é explicada em detalhes no capítulo **Plugins**.

© Aker Security Solutions

Diferentemente das outras filtragens por política, a filtragem de Spam Meter, por sua própria característica, só está disponível para e-mails de entrada, ou seja, enviados por remetentes externos à rede protegida pelo ASMG.

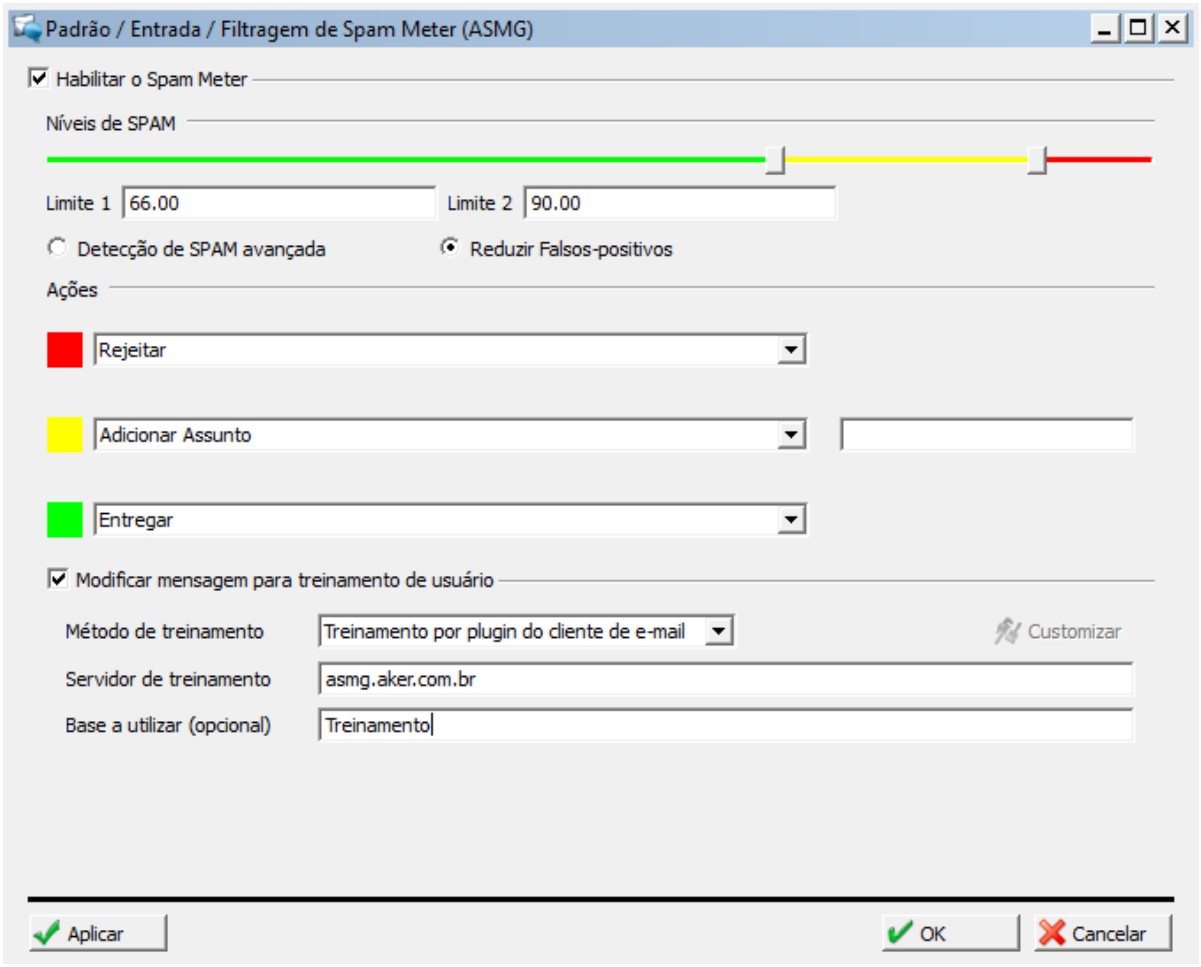

Figura 102. Filtragem do Spam Meter.

Configurando o Mecanismo de Classificação e Filtragem de Mensagens

A primeira opção desta janela se refere à habilitação da filtragem. Uma vez habilitada, os demais campos de configuração ficarão disponíveis para edição.

Logo abaixo, existe o objeto de configuração dos limiares para cada nível de pontuação. Esta configuração pode ser feita a partir do objeto gráfico, com o auxílio do mouse, ou então a partir dos campos que guardam as porcentagens de cada nível. Como o SPAM é um conceito abstrato, o ASMG permite que o administrador defina ele próprio, em três níveis, as probabilidades de um e-mail ser considerado SPAM, assim como as ações a serem tomadas para cada um desses níveis. O nível verde deve ser utilizado para representar a faixa de pontuação de mensagens não consideradas SPAM. Por exemplo, se ele escolher o valor de 50%, está dizendo que mensagens classificadas com probabilidades de até 50% não são consideradas SPAM pelo seu domínio. O nível amarelo deve ser utilizado para definir a faixa de mensagens que serão consideradas provavelmente SPAM e, finalmente, o nível

vermelho deve ser utilizado para definir a faixa de pontuação que deve ser tratada com SPAM para o domínio.

As opções "Detecção de SPAM avançada" e "Reduzir Falso-positivos, mutuamente exclusivas, definem o tipo de algoritmo a ser empregado para a classificação. A primeira opção, apesar de um pouco mais eficiente, pode ter um desempenho um pouco inferior que a segunda.

Para a configuração da ação, o administrador pode escolher, para cada um dos três níveis, o comportamento desejado para a filtragem. As opções são:

- Entregar;
- Rejeitar;
- Rejeitar a mensagem e copiar para Quarentena;
- Rejeitar a mensagem e enviar para uma lista de endereços;
- Adicionar Assunto;
- Rejeitar a mensagem, copiar para Quarentena e enviar para uma lista de endereços.

Configurando o Treinamento de Mensagens

A operação de treinamento é de importância vital para a personalização da filtragem de Spam Meter para os perfis dos usuários que compõem a empresa protegida pelo ASMG. É a partir deste procedimento que a filtragem vai conseguir refletir o sentimento de cada departamento da empresa com relação a mensagens de SPAM, pois os próprios usuários terão a oportunidade de definir as características de mensagens que eles consideram SPAM e as características daquelas que não consideram SPAM.

Como a filtragem é diferenciada para cada política, o administrador vai poder definir quais são as políticas que poderão fazer o treinamento e, mais interessante ainda, definir diferentes bases para cada uma delas, de modo que a empresa tenha ao final diferentes bases de conhecimento a respeito de SPAM, adequadas a diferentes perfis de pessoas.

O procedimento de treinamento é extremamente simples. Tudo que o usuário precisa fazer é clicar num botão, o qual será inserido nas mensagens que ele recebe. Na verdade, serão inseridos dois botões: um deles para ser utilizado pelo usuário para que ele defina a mensagem como SPAM; e um segundo para que classifique a mensagem como não sendo um SPAM.

Para habilitar o treinamento de mensagens para a política em questão, o administrador deve, antes de tudo, deixar marcada a opção "Modificar mensagem para treinamento de usuário". O próximo passo é a escolha do método de treinamento desejado. As opções disponíveis são:

- Treinamento por plugin do cliente de e-mail

© Aker Security Solutions

Para esta opção, o ASMG não modifica o conteúdo da mensagem original, porém, altera seu código fonte (cabeçalho). Contudo, deve ser instalado no cliente de e-mail dos computadores dos usuários um plugin, o qual propiciará as opções de treinamento. Este plugin é gratuito e pode ser obtido no site da Aker. Atualmente, ele oferece suporte para os clientes de e-mail Microsoft Outlook, Mozilla Thunderbird.

- Treinamento por HTML

Neste caso, o ASMG enviará em anexo HTML contendo as informações necessárias para o treinamento. Para esta opção, não há necessidade de instalação do plugin. Contudo, o cliente de e-mail utilizado pelo usuário da rede deverá ter um suporte completo a código HTML embutido em mensagens eletrônicas.

- Treinamento no corpo da mensagem

Neste caso, o ASMG modificará o código fonte da mensagem original, inserindo no final do corpo do e-mail as informações de treinamento. Para esta opção, não há necessidade de instalação do plugin.

O botão "Customizar" permite ao administrador definir os textos que irão compor as versões modificadas das mensagens, caso se opte pela segunda ou terceira opção de treinamento.

O próximo parâmetro, "Servidor de treinamento", deve ser preenchido com as informações de endereço IP ou nome do servidor onde é executado o ASMG, a fim de que as informações de treinamento dos usuários sejam encaminhadas por ele para o ASM.

Finalmente, através do parâmetro "Base a utilizar (opcional)", o administrador poderá definir, para cada política, o nome da base a ser utilizada nas operações de treinamento e classificação. Se este campo não for preenchido, o ASMG irá gerar um nome padrão de base.

© Aker Security Solutions

Número Máximo de Mensagens

Esta janela permite ao usuário através de uma política, limitar o número máximo de mensagens em um determinado período de tempo.

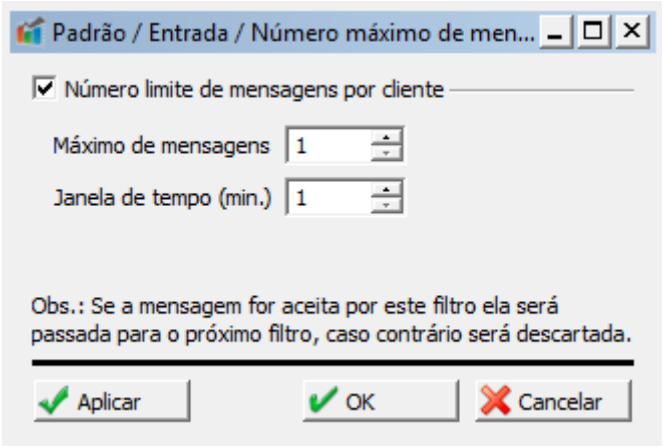
Padrão / Entrada / Número máximo de men...
Número limite de mensagens por cliente
Máximo de mensagens
1
Janela de tempo (min.)
1
Obs.: Se a mensagem for aceita por este filtro ela será passada para o próximo filtro, caso contrário será descartada.
Aplicar
OK
Cancelar

Figura 103. Número máximo de mensagens.

A opção "Limitar o número de mensagens por cliente" permite ao usuário definir uma quantidade máxima de mensagens que serão recebidas em um determinado período de tempo.

Por exemplo: Se o número "Máximo de mensagens" for 10 e o tempo definido for 5 minutos, significa que no período de 5 minutos serão recebidas no máximo 10 mensagens.

Tamanho Máximo

Tanto as mensagens que chegam quanto as que saem possuem as mesmas características quanto à restrição: é possível restringir o tamanho máximo da mensagem como um todo (em KB), apenas seus anexos (também em KB) ou a ambos.

Caso este filtro esteja habilitado, sempre que uma mensagem, anexo ou conjunto mensagem/anexo ultrapassar o tamanho máximo estipulado, terá seu conteúdo removido e substituído por uma mensagem do sistema.

Adicionalmente, podemos encaminhar as mensagens limitadas por estas regras para algum endereço de e-mail previamente cadastrado, ou ainda, mover estas mensagens para a quarentena para posterior análise.

© Aker Security Solutions

Entrada

Nesta tela restringimos os tamanhos das mensagens que chegam para os usuários internos (destinatários).

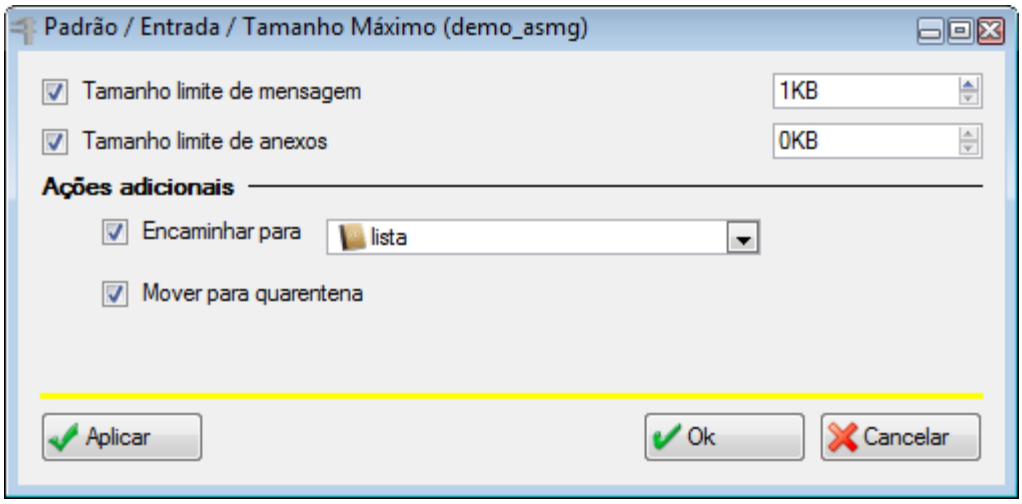

Figura 104. Tamanho máximo de mensagens.

Os parâmetros possíveis de serem configurados são os seguintes:

- **Tamanho limite de mensagem:** se marcada, podemos definir o tamanho máximo, em KB, que a mensagem (incluindo anexos) pode ter;
- **Tamanho limite de anexos:** se esta opção for marcada, podemos definir o tamanho máximo, em KB, que os anexos de uma mensagem podem ter.

Além disso, podemos definir que a mensagem seja encaminhada para algum e-mail específico e/ou movida para quarentena.

Saída

Nesta tela restringimos os tamanhos das mensagens que são enviadas pelos usuários internos (remetentes). Caso o anexo ou a mensagem ultrapasse o limite estabelecido, serão descartados e o remetente recebe uma mensagem informativa, conforme mencionado no capítulo **Mensagens de Notificação**.

As configurações para o tamanho das mensagens enviadas são inseridas da mesma maneira que as das mensagens são consideradas de **Entrada**.

Tipos de Arquivos

O ASMG permite definir se um anexo será aceito ou não, de acordo com o seu tipo. Estes anexos são entidades do tipo "Arquivos" já previamente cadastrados, e serão analisados quanto a seu tipo real.

O **ASMG** já vem pré-configurado com os tipos de arquivos mais comuns. Entretanto, caso o usuário necessite de filtragem para um tipo de arquivo não cadastrado, pode cadastrá-lo sem qualquer restrição.

Nas “Ação” do filtro você decide se quer manter os anexos listados na janela e remover os que não estão, ou remover os anexos listados na janela e manter os não listados.

Uma mensagem de notificação será colocada na mensagem, informando ao destinatário que ali havia um arquivo anexado e que ele foi retirado.

Entrada

Nesta tela configuramos as restrições de arquivos quem chegam aos usuários internos (destinatários). Na figura abaixo, selecionamos dois tipos de arquivo, "bat" e "exe" que estão sendo removidos, e encaminhados automaticamente para a quarentena. Estes dois arquivos estão relacionados como exemplo, pois, com freqüência, estes tipos de anexo representam vírus e, por isso, devem ser mais bem analisados.

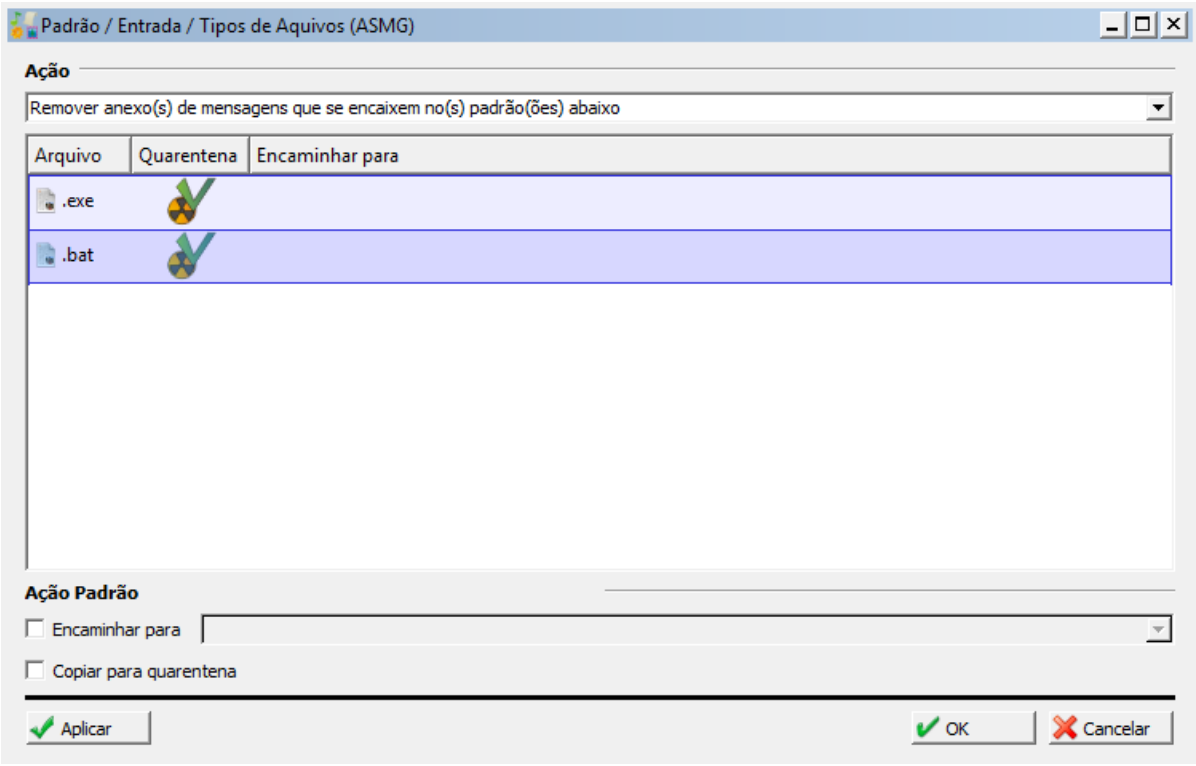

Figura 105. Entrada – tipos de arquivos.

Para realizar esta configuração, basta fazer o seguinte:

- Clique com o botão direito do mouse em qualquer lugar do quadro e escolha a opção **"Inserir";**
- Em seguida, clique com o botão direito do mouse sob a coluna **"Arquivo"** e escolha a opção **"Adicionar Entidades"**;
- Selecione a entidade do tipo "Arquivo" que deseja que seja adicionada à regra. Clique em **"Adicionar"**;
- Para indicar se a mensagem deve ir para a quarentena ou não, clique com o botão direito do mouse sob a coluna **"Quarentena"** e escolha entre as opções **"Habilitar"** ou **"Desabilitar"**;
- Se desejar encaminhar uma cópia da mensagem para alguém, clique com o botão direito do mouse sob a coluna **"Encaminhar para"**, selecione a opção **"Adicionar Entidades"** e escolha a entidade do tipo "Lista de E-mail" desejada. Clique em **"Adicionar"**.

Saída

Nesta tela configuramos as restrições de arquivos que são enviados pelos usuários internos (remetentes).

Para adicionar arquivos que deverão ser analisados quando enviados por usuários internos, basta seguir os mesmos passos indicados para analisar arquivos que chegam da Internet. A diferença aqui é que quando configuramos a ação, pedimos que anexos que contivessem arquivos executáveis fossem descartados. Neste caso, o remetente recebe uma mensagem informando que o anexo foi removido, conforme explicado no capítulo Mensagens de Notificação.

© Aker Security Solutions

Whitelist/Blacklist

Esta configuração definirá quais e-mails ou domínios farão parte de uma whitelist ou blacklist. Isto significa que o e-mail/domínio que estiver em uma whitelist não será bloqueado por nenhum filtro desta política e o e-mail/domínio que estiver em uma blacklist será bloqueado.

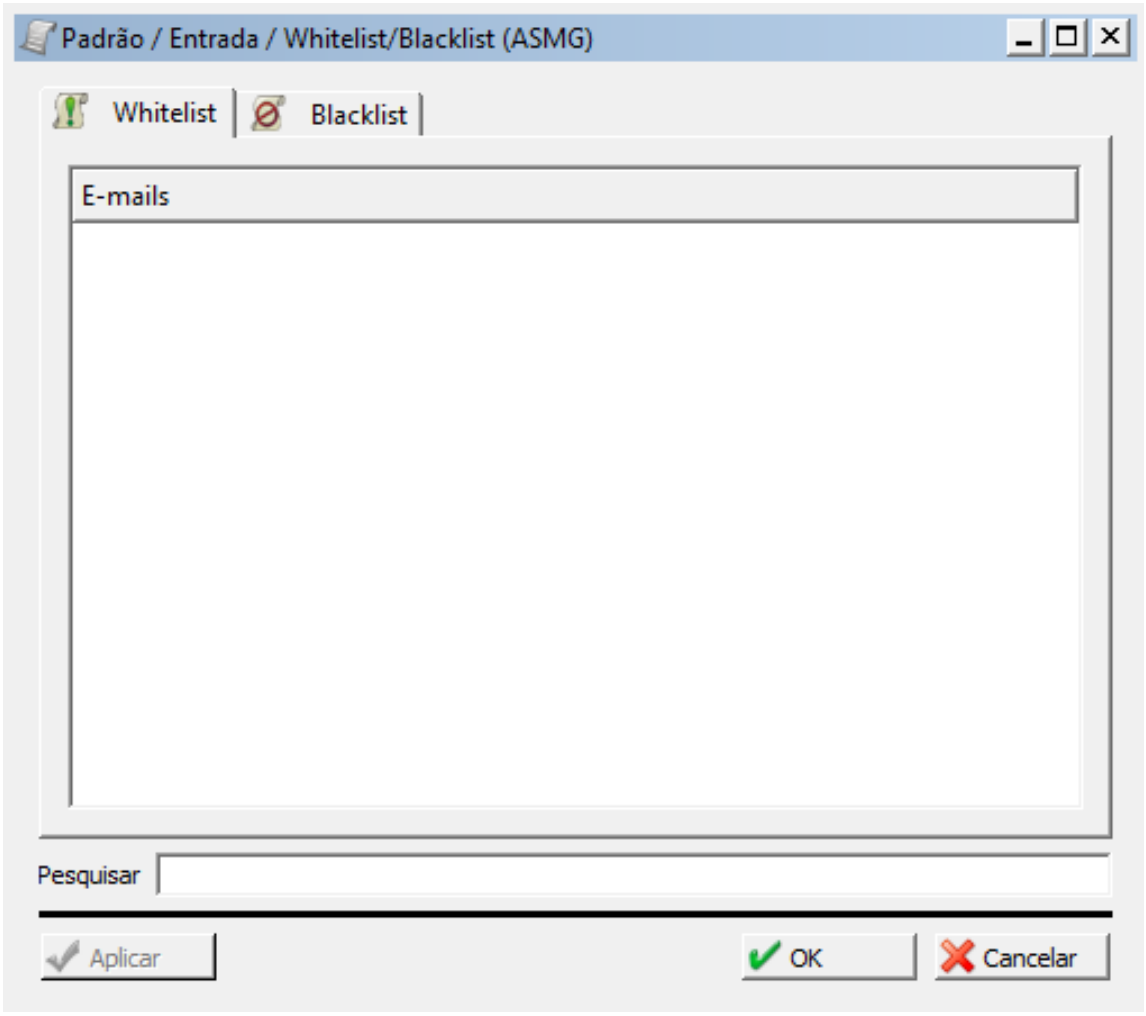

Figura 106. Entrada – whitelist e blacklist.

© Aker Security Solutions

Ordenação de Filtro

Esta configuração definirá em qual ordem os filtros de uma política serão executados, ou seja, definindo qual filtro será mais prioritário naquela política.

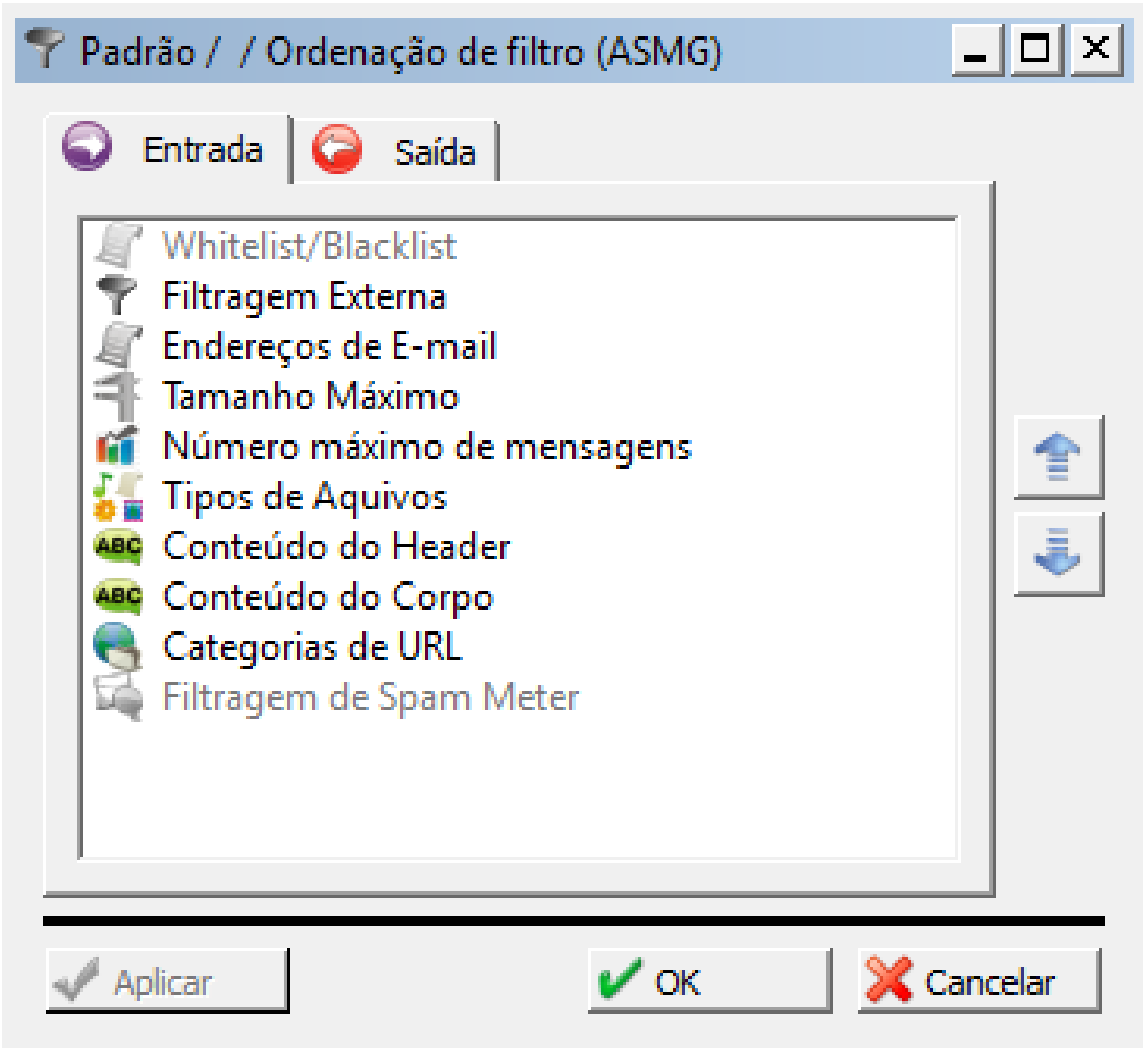

Figura 107. Ordenação de filtro.

Relatórios

14. Relatórios

Esta parte da configuração permite configurar a geração automática e agendada de relatórios e ainda gerar em tempo real todos os relatórios oferecidos pelo ASMG. Os relatórios do ASMG compreendem arquivos HTML que apresentam gráficos, de pizza e de linha, com os devidos dados relacionados, além de tabelas com os dados em números absolutos e outros parâmetros de cabeçalho de relatório, como data e logo da empresa. O produto oferece os seguintes tipos de relatórios:

- Maiores ocorrências de remetentes;
- Maiores ocorrências de destinatários;
- Maiores ocorrências de domínios dos remetentes;
- Maiores ocorrências de tipos de Arquivos;
- Maiores ocorrências de vírus em anexos;
- Mensagens Aceitas e Rejeitadas;
- Ocorrências por Filtros Aplicados.

A seguir explicaremos cada um desses relatórios e também falaremos sobre o agendamento de relatórios.

Configurações de Relatórios

Esta janela armazena os parâmetros de configuração do sistema de relatórios do ASMG. Ela também gerencia a questão dos relatórios agendados, propiciando o cadastro do agendamento e configuração de todos os parâmetros relacionados.

© Aker Security Solutions

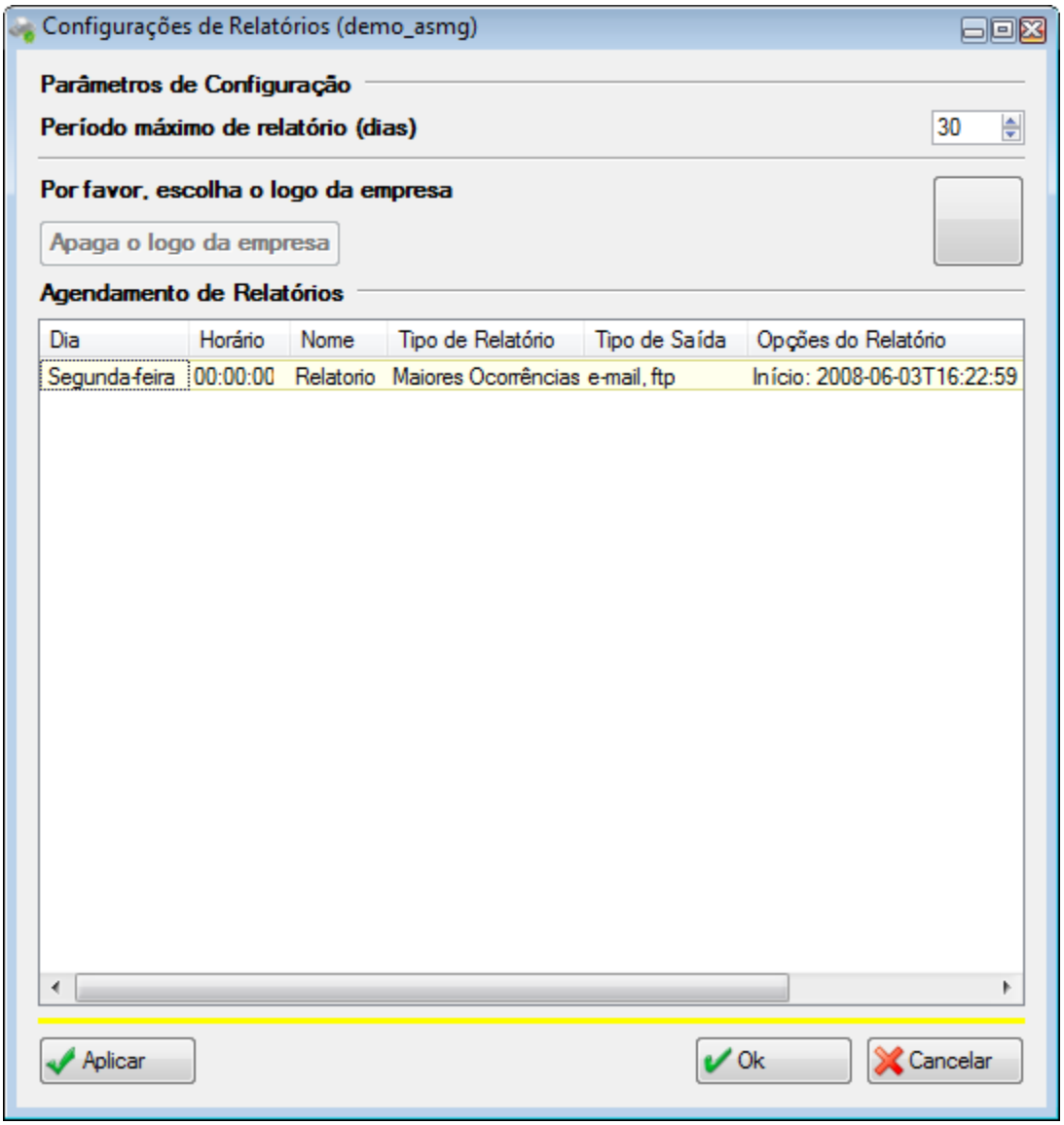

Figura 108. Configuração de relatórios.

O primeiro parâmetro desta janela define o número de dias que o produto ficará guardando informações de log. O valor é definido em dias. Para os dados de relatórios mais antigos do que o tempo definido neste controle, o ASMG remove os arquivos correspondentes.

A segunda opção da janela permite ao administrador da rede carregar a figura de logo da empresa. Esta figura será utilizada nos relatórios, caso seja necessário e assim definido pelo administrador, individualmente para cada relatório. É oferecido o suporte a figuras do tipo JPG e PNG.

Agendamento de Relatórios

Para criar um relatório agendado é necessário clicar com o botão direito do mouse sobre a lista de relatórios, selecionando a opção "Novo". Será mostrada uma nova janela, com todos os parâmetros disponíveis para a criação de um relatório.

© Aker Security Solutions

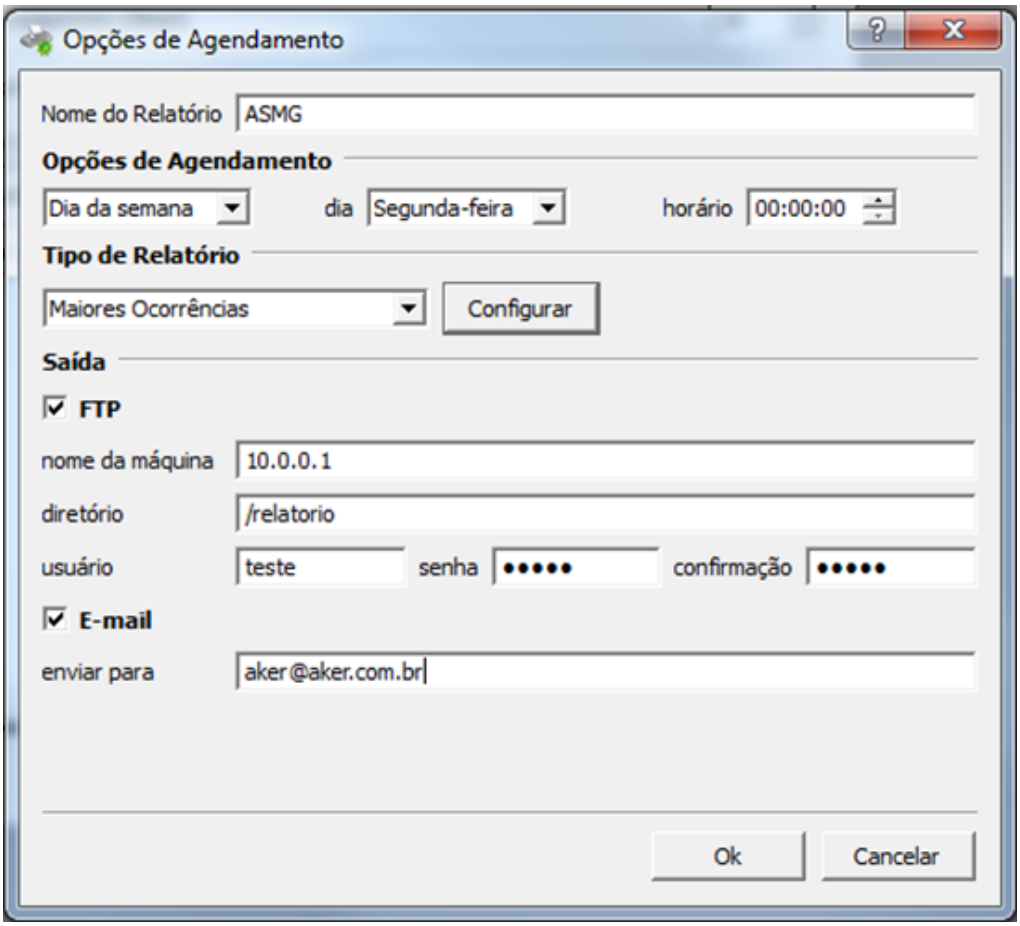

Figura 109. Opções de agendamento.

O primeiro parâmetro do relatório agendado a ser definido é a opção de agendamento. Os relatórios do ASMG são agendados com periodicidade semanal ou mensal e sua execução é repetida a cada semana ou a cada mês, dependendo do que for escolhido. Após escolher o tipo de geração (semanal ou mensal), é necessário escolher o dia da semana (ou dia do mês) e o horário em que a geração do relatório deve ser disparada.

Com relação ao tipo de relatório é necessário escolher o relatório desejado e, a seguir, definir os parâmetros do tipo escolhido, clicando no botão "Configurar". Ao fazer isso, será aberta uma nova janela para que sejam definidos os parâmetros do relatório propriamente dito. Para maiores detalhes cm relação a esses parâmetros, consulte as subseções abaixo.

Finalmente, a última configuração do agendamento é selecionar o tipo de saída desejado. O ASMG permite três tipos de saída, que podem inclusive serem utilizados simultaneamente:

- **FTP**

O ASMG neste caso envia os arquivos de relatório para um site de FTP. Neste caso, é necessário configurar os detalhes da conexão FTP a ser estabelecida

oportunamente. São eles: nome da máquina ou endereço IP do servidor FTP, diretório do servidor FTP onde devem ser colocados os arquivos de relatório, usuário do site FTP e sua senha.

- **E-mail**

Caso esta opção seja selecionada, o ASMG irá enviar, por e-mail, os arquivos do relatório para um endereço configurável.

Após as configurações, basta clicar no botão **"OK"** para as opções de agendamentos serem configuradas.

© Aker Security Solutions

Repositórios

15. Repositórios

Repositórios são espaços alocados em disco, onde o **ASMG** armazena as mensagens enquanto executa seu processamento. Estes repositórios são dinâmicos, tendo em vista que as mensagens que trafegam por eles são apenas transitórias e logo serão encaminhadas para o servidor pertinente ou então descartadas.

Este item está subdividido em duas áreas distintas. São elas:

- Repositório de Quarentena;
- Repositório de Sistema.

A seguir descreveremos detalhadamente a diferença entre as duas áreas.

Repositório de Quarentena

Esta janela oferece o gerenciamento do repositório de quarentena. Apesar de também ser um repositório temporário de mensagens, seu objeto de controle são as mensagens que, em qualquer uma das janelas de filtragem, foram configuradas para serem enviadas para quarentena. Este repositório não permite a limitação de tamanho máximo e número de arquivos. Sua configuração limita-se à especificação do diretório para armazenamento de mensagens.

A quarentena deve ser utilizada pelo Administrador para mensagens que fogem de um determinado padrão a ponto de merecerem ser visualizadas ou analisadas manualmente. Para cada política criada, é possível determinar o tempo máximo de quarentena para as mensagens armazenadas. Se ao fim desse período nenhuma operação for realizada, as mensagens são automaticamente eliminadas.

A seguir explicaremos as funções das abas "Visualizador" e "Configurações" e como estas devem ser manipuladas.

Aba Visualizador

Nesta aba o Administrador gerencia as mensagens que estão em quarentena. Aqui podemos visualizar as mensagens enviadas para a quarentena, removê-las manualmente, enfileirá-las novamente ou acessar seu código fonte.

© Aker Security Solutions

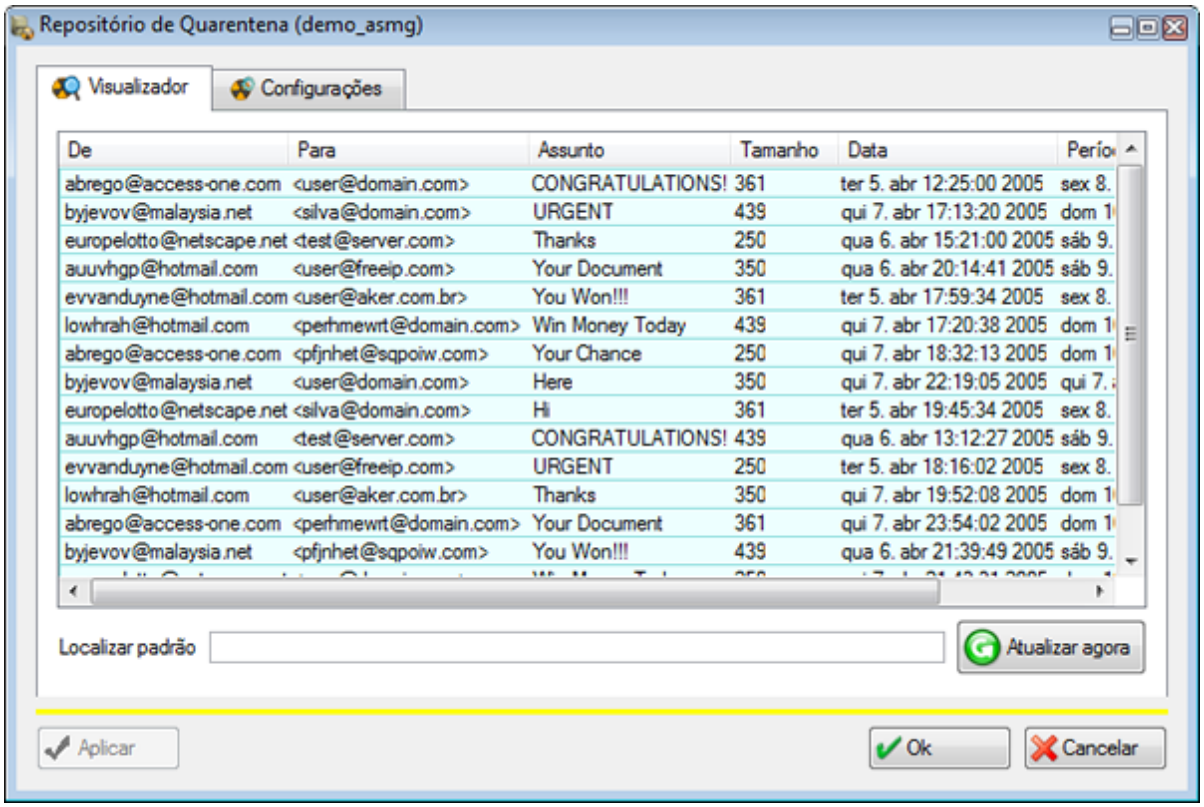

Figura 110. Repositório de quarentena.

Conforme mencionado anteriormente, podemos realizar uma série de operações com as mensagens armazenadas no Repositório de Quarentena. Os botões se encontram na barra superior, conforme imagem abaixo:

Figura 111. Barra dos botões de operações - Repositório de quarentena.

Na ordem dos botões (da direita para esquerda):

- **Re-enfileirar:** basta clicar sobre o botão **"Reenfileirar"**, localizado na barra de ferramentas do Aker Control Center;
- **Remover manualmente:** basta selecionar a mensagem lista de mensagens em quarentena e clicar sobre o botão **"Remover"**, localizado na barra de ferramentas do Aker Control Center;
- **Visualizar o código fonte:** selecione a mensagem dentro da lista de mensagens em quarentena e, em seguida, clique sobre o botão **"**Mostrar Fonte", localizado na barra de ferramentas do Aker Control Center.
- **Treina mensagem como Não SPAM**: selecione a mensagem dentro da lista de mensagens em quarentena e, em seguida, clique sobre o botão, opção disponível quando integrado com o Aker Spam Meter;

© Aker Security Solutions

- **Treina mensagem como SPAM:** selecione a mensagem dentro da lista de mensagens em quarentena e, em seguida, clique sobre o botão, opção disponível quando integrado com o Aker Spam Meter;
- **Enviar e-mail para Whitelist Global:** selecione a mensagem dentro da lista de mensagens em quarentena e, em seguida, clique sobre o botão, o endereço de e-mail do remetente será inserido na Whitelist Global do ASMG;
- **Enviar e-mail para Blacklist Global:** selecione a mensagem dentro da lista de mensagens em quarentena e, em seguida, clique sobre o botão, o endereço de e-mail do remetente será inserido na Blacklist Global do ASMG;
- **Habilitar refresh automático**: atualiza a lista de e-mails na quarentena no tempo determinado.

Já na janela de visualização temos a opção:

- **Pesquisa:** basta digitar uma string no campo **"Localizar Padrão"** e, em seguida, clicar sobre o botão **"Atualizar Agora".** A busca acontece nos campos "De", "Para" e "Assunto" da mensagem;

Aba Configurações

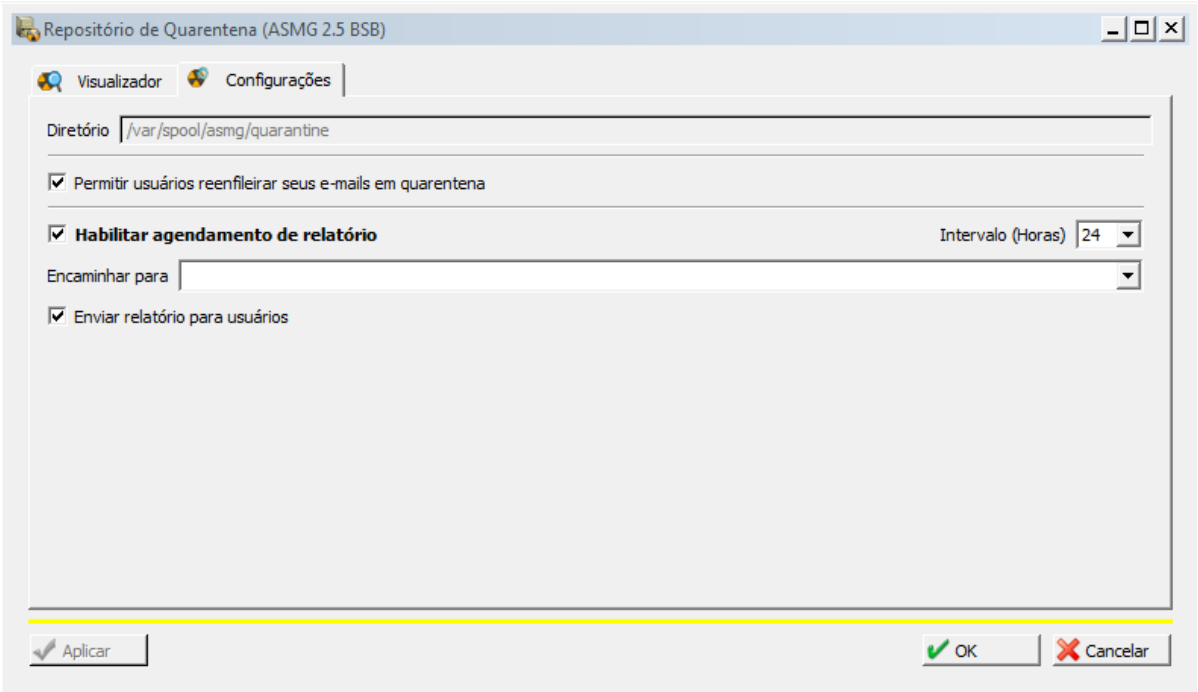

Figura 112. Repositório de quarentena - configurações.

Nesta aba, devemos informar o local onde as mensagens em quarentena devem ser armazenadas e o envio de relatórios conforme opções abaixo:

- **Diretório:** local onde as mensagens em quarentena devem ser armazenadas;
- **Permitir usuários reenfileirar seus e-mails em quarentena:** utilizando à Webgui (veja capítulo **Interface Gráfica do Usuário**);

- Habilitar agendamento de relatório:
- **Intervalo (Horas):** intervalo de tempo em horas que o ASMG encaminhará relatórios aos destinatários de sua lista de e-mails em quarentena;
- **Encaminhar para**: lista de e-mail(s) que será enviado relatório de e-mails em quarentena;
- **Enviar relatório para usuários**: define que os usuários receberão a lista de seus e-mails em quarentena.

Repositório de Sistema

O processamento pelo **ASMG** é dividido em três momentos distintos: recebimento, processamento e a finalização, que pode ser o encaminhamento da mensagem para seu destinatário final, armazenamento para análise futura ou então o descarte. Durante cada uma destas fases, o sistema armazena as mensagens em diretórios específicos enquanto aguarda a conclusão de uma etapa para só então prosseguir para a seguinte.

Os repositórios de sistema são compostos por *File Keepers*, ou seja, mantenedores de arquivos utilizados pelo **ASMG** para promover o armazenamento temporário de mensagens em diretórios específicos, em etapas também específicas do processamento.

A seguir explicaremos sobre os tipos de Repositório de Sistema, as funções de cada um e as informações necessárias para configurá-los.

Aba "Serviço Inbound"

Nesta aba, temos as informações sobre o armazenamento temporário das mensagens assim que são recebidas pelo programa, antes que ele execute qualquer operação relativa a elas.

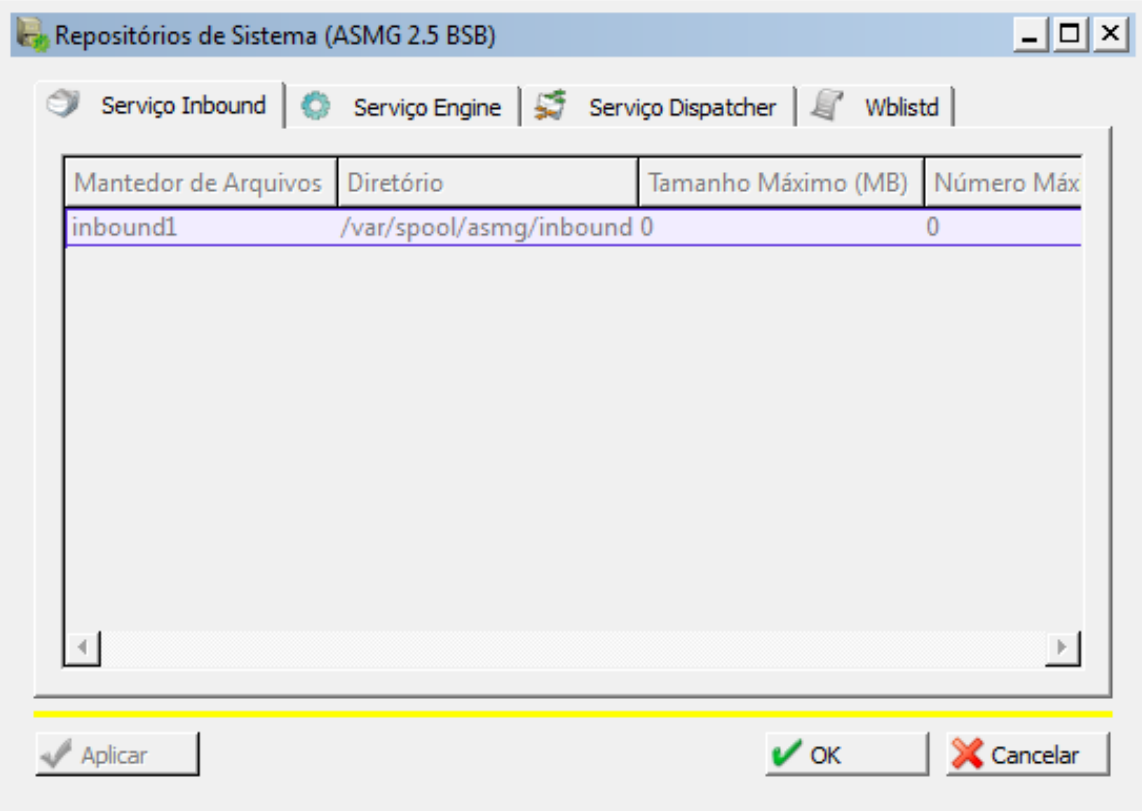

Figura 113. Repositório de sistema – Serviço inbound.

Aba "Serviço Engine"

Aqui visualizamos as informações sobre o armazenamento temporário das mensagens enquanto elas passam por todo o processo de filtragem de dados.

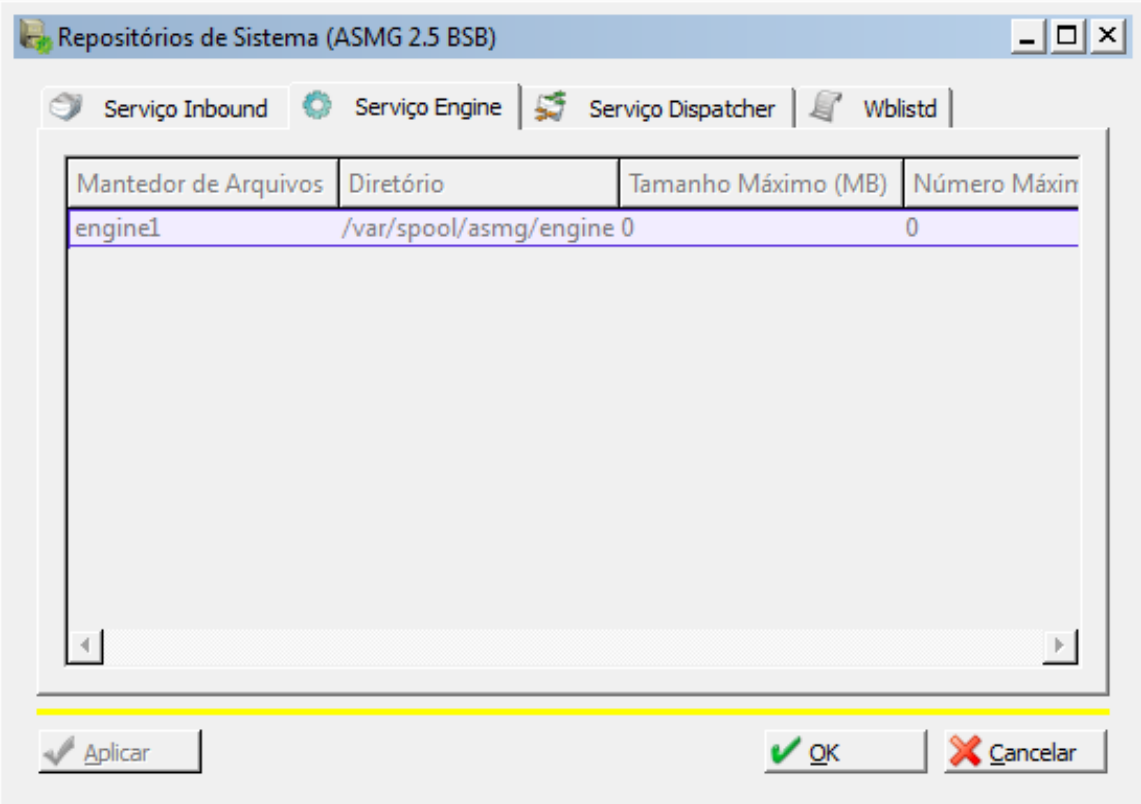

Figura 114. Repositório de sistema – Serviço engine.

Aba "Serviço Dispatcher"

Nesta aba verificamos as informações relativas ao armazenamento temporário das mensagens que estão sendo encaminhadas.

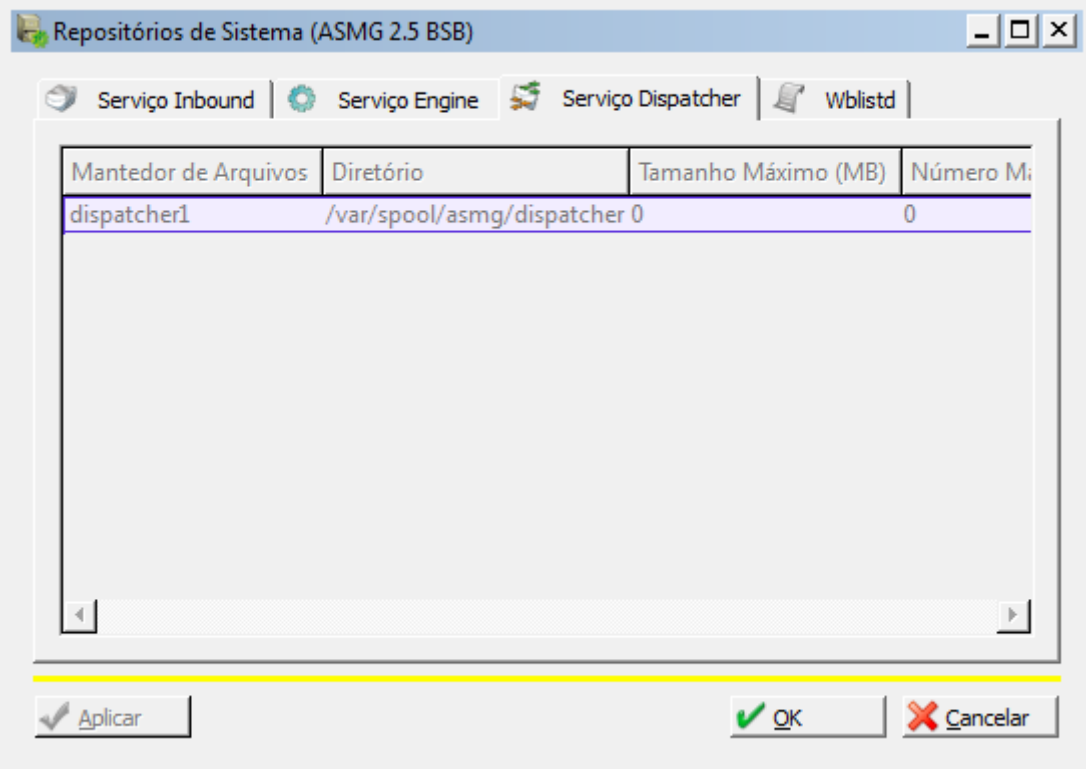

Figura 115. Repositório de sistema – Serviço Dispatcher.

Aba "Serviço Wblistd"

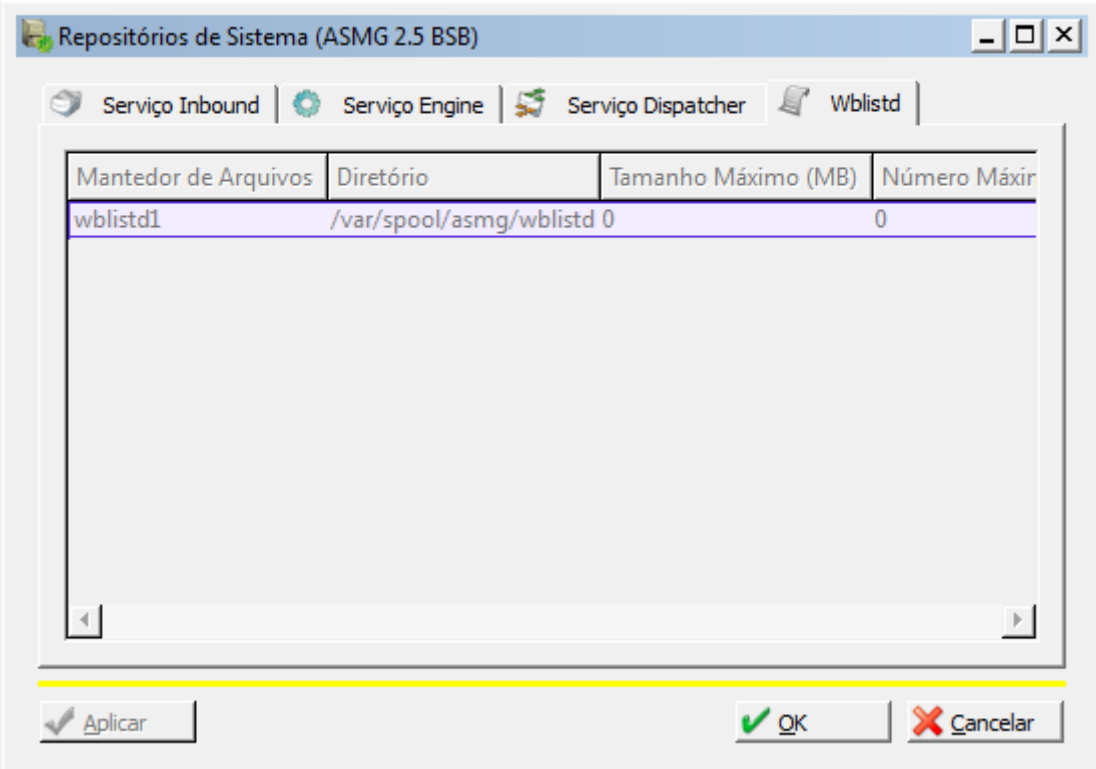

Figura 116. Repositório de sistema – Wblistd.

Conforme demonstrado nas figuras anteriores, as informações necessárias para configurar cada aba são basicamente as mesmas. O que deve ser levado em consideração é o papel de cada uma no **ASMG**. Dentro das telas existem os seguintes parâmetros a ser definidos:

- Mantenedor de arquivos: informar o nome do File Keeper;
- Diretório: endereço completo de armazenamento das mensagens;
- Tamanho Máximo: máximo de espaço em disco, em MB, que o diretório pode ocupar. Se o campo não for preenchido, o tamanho máximo é ilimitado;
- Número Máximo de Arquivos: quantidade máxima de arquivos que pode ser armazenada simultaneamente. Se o campo não for preenchido, o número máximo é ilimitado.

Com o intuito de facilitar a administração do sistema, os *file keepers* já vêm pré-configurados e, por isso, certas alterações como limitação de número de arquivos armazenados, limitação de espaço em disco ou mudança do diretório só devem ser feitas em casos muito específicos. Para esclarecimento, vamos demonstrar como é feita a configuração manual da aba, tomando como exemplo a configuração da aba **"Serviço Dispatcher"**.

- Clique com o botão direito do mouse em qualquer lugar do quadro e escolha a opção **"Inserir"**;
- Localize a coluna **"Mantedor de Arquivos"**, clique com o botão direito do mouse abaixo dela e digite o nome escolhido. No nosso exemplo, escolhemos o nome *dispatcher1*;
- A seguir, clique o botão direito do mouse abaixo da coluna "Diretório" e informe o caminho completo de armazenamento. No nosso exemplo, o caminho é /var/aker/dispatcher, mas esta definição fica a cargo do Administrador;
- As colunas **"Tamanho máximo (MB)"** e **"Número Máximo de Arquivos"** têm o preenchimento opcional. Se desejar inserir dados, basta clicar com o botão direito do mouse abaixo de cada uma delas e digitar o tamanho alocado em disco e a quantidade máxima de arquivos.

© Aker Security Solutions

Entidades

16. Entidades

Na **Programação Orientada a Objeto (POO)**, definimos Entidades como representações lógicas de objetos que existem no mundo real. No **ASMG**, este conceito é amplamente utilizado para facilitar o gerenciamento do produto, pois podemos agrupar em uma mesma Entidade objetos que possuem as mesmas características, mas que possuem aplicações diferentes. Por exemplo: através da Entidade “Lista de E-mails” podemos criar uma lista de e-mails de remetentes que serão automaticamente bloqueados para envio de mensagens para a rede interna (*blacklist*) e outra de remetentes que serão automaticamente autorizados a enviar mensagens para a rede interna (*whitelist*). Podemos ver que o objeto é o mesmo: uma lista de e-mails. No entanto, a aplicação destes dois objetos é totalmente diferente.

As entidades são facilmente configuráveis e estão separadas nas seguintes categorias:

- **Servidores:** entidade que armazena endereços IP de servidores que serão instanciados em diferentes áreas do **ASMG;**
- **Domínios:** entidade que armazena os domínios que serão instanciados dentro do **ASMG;**
- **Lista de Domínios:** entidade que armazena uma lista de domínios que serão instanciados dentro do **ASMG**
- **Redes:** entidade que armazena endereços e máscaras de redes que serão instanciadas dentro do **ASMG**;
- **RBLs:** listas externas que contêm relações de servidores de e-mail promíscuos (*open relay)* comumente utilizados por spammers;
- **Listas de E-mail:** grupos de endereços que serão utilizados em diversas ações e filtragens executadas pelo **ASMG**;
- **Listas de Palavras-chave:** análogas às listas anteriores, também são listas de palavras de interesse, que alimentarão os filtros do **ASMG**;
- **Listas de Expressão Regular:** listas de expressões de interesse (comuns em spams, por exemplo) que alimentarão os filtros do **ASMG**;
- **Autenticadores:** através desta entidade, podemos estabelecer autenticadores externos para validar usuários pertencentes à rede onde o **ASMG** está instalado;
- **Arquivos:** descrição de tipos de arquivos que serão utilizados pelos filtros do **ASMG**;
- **Filtros externos:** integração entre o **ASMG** e scripts ou programas externos para filtrar mensagens.

© Aker Security Solutions

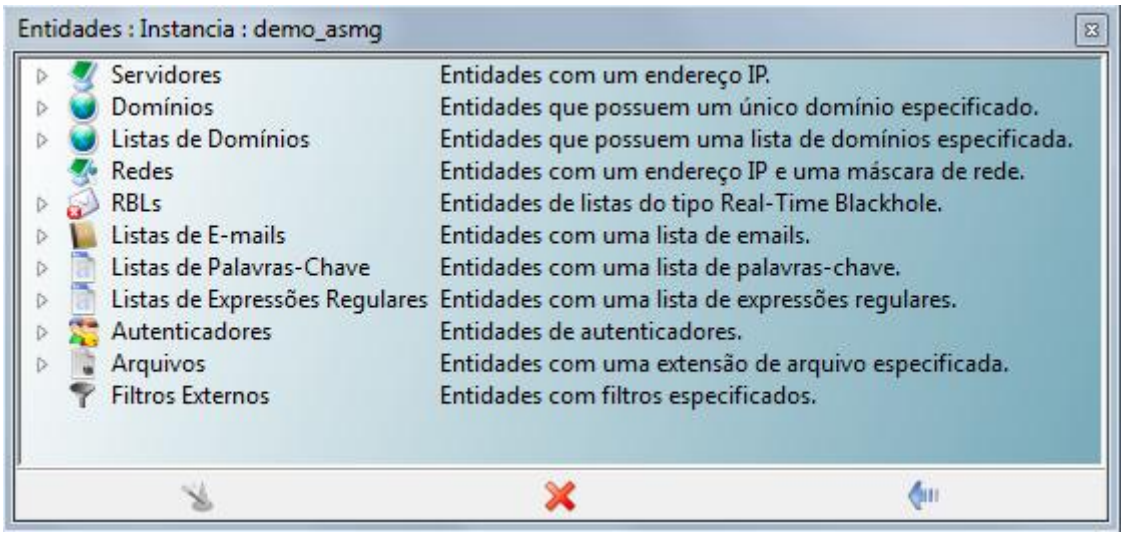
Entidades : Instancia : demo_asmg
Servidores
Entidades com um endereço IP.
Domínios
Entidades que possuem um único domínio especificado.
Listas de Domínios
Entidades que possuem uma lista de domínios especificada.
Redes
Entidades com um endereço IP e uma máscara de rede.
RBLs
Entidades de listas do tipo Real-Time Blackhole.
Listas de E-mails
Entidades com uma lista de emails.
Listas de Palavras-Chave
Entidades com uma lista de palavras-chave.
Listas de Expressões Regulares
Entidades com uma lista de expressões regulares.
Autenticadores
Entidades de autenticadores.
Arquivos
Entidades com uma extensão de arquivo especificada.
Filtros Externos
Entidades com filtros especificados.

Figura 117. Configuração das entidades.

Configurando As Entidades

Conforme dito anteriormente, as entidades mantêm parâmetros e valores que serão amplamente utilizados na operação do **ASMG**. Considerando a importância e versatilidade dos papéis que elas desempenham, é muito importante entender como manuseá-las e parametrizá-las.

Por esta ser uma ferramenta facilmente customizável, o acréscimo ou retirada de informações podem ser feitos de maneira simples, sempre que necessário. É importante lembrar que certas configurações devem ser bem estudadas a fim de não se chocarem, o que impediria a obtenção do resultado desejado.

Para ter acesso à janela que contém as Entidades, abra o **Aker Control Center** e conecte-se ao dispositivo a ser gerenciado. Em seguida, clique no menu **"Janelas"** e selecione **"Entidades"**. Esta nova janela pode ser posicionada em vários lugares da tela, cabendo ao usuário do sistema definir qual o melhor local.

A seguir, vamos descrever as Entidades uma a uma, informando a maneira como elas podem ser acessadas e ter dados inseridos.

Arquivos

É possível configurar tipos de arquivos que serão ignorados durante a filtragem de conteúdo. Dependendo do tipo de política adotada pela empresa, será possível filtrar anexos que contenham imagens, sons, filmes, etc.

© Aker Security Solutions

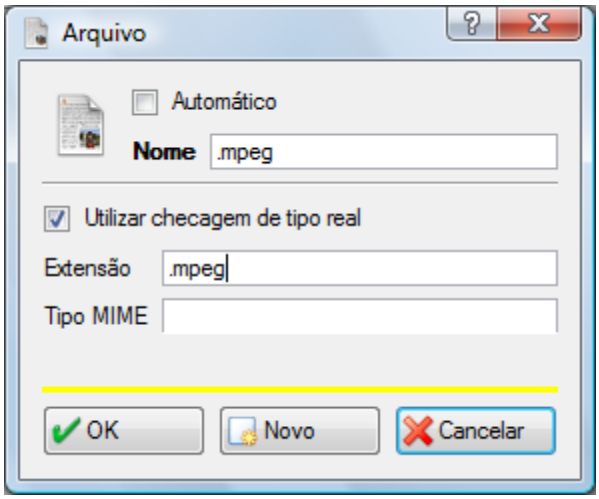

Figura 118. Configuração dos tipos de arquivos.

O **ASMG** já fornece na instalação um conjunto de Entidades do tipo “Arquivos” pré-criado que, por sua vez, representam os tipos de arquivos mais comuns. Caso o Administrador deseje adicionar novas Entidades do tipo “Arquivo”, basta proceder da seguinte maneira:

- Clique com o botão direito do mouse sobre a entidade **“Arquivos”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar ao filtro na caixa **“Nome”**, ou marque a opção **“Automático”**;
- Preencha os campos com as informações de Extensão, Tipo Real e Tipo MIME, e clique em **OK**;
- Caso deseje adicionar mais entidades do tipo “Arquivo”, repita os passos de 1 a 4, quantas vezes forem necessárias.

Autenticadores

Esta entidade representa um agente de autenticação Aker, um programa especializado em servir como meio de comunicação entre uma base de dados que possui o cadastro de usuários e grupos da rede e o **ASMG**.

O **ASMG** necessita dessa base de dados de usuários para efetuar operações tais como: descoberta de grupos aos quais um usuário pertence ou autenticação de um usuário da rede na interface do usuário.

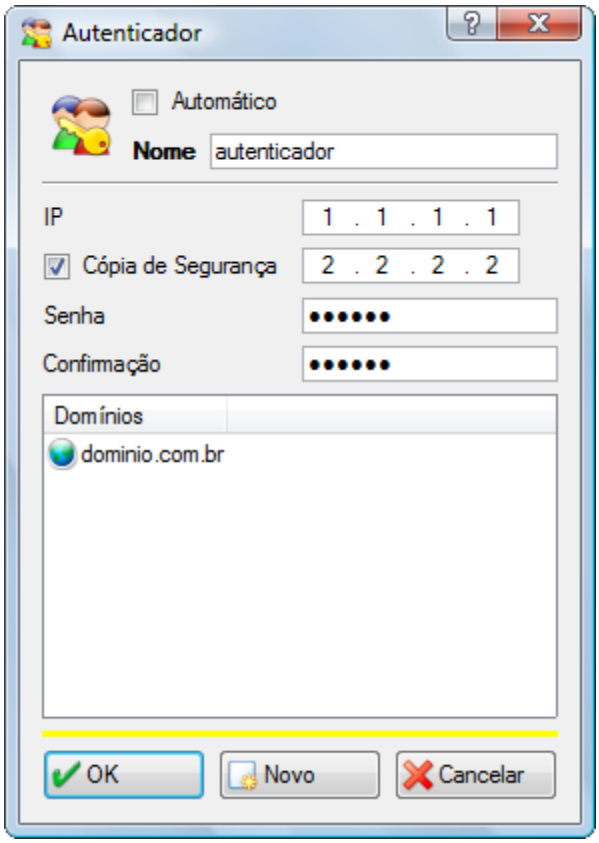

Figura 119. Adicionar entidades.

Para que possamos adicionar uma Entidade do tipo “Autenticadores”, siga estes passos:

- Clique com o botão direito do mouse sobre a entidade **“Autenticadores”**;
- Selecione a opção **“Novo”**;
- Na tela seguinte, digite o nome que deseja dar ao autenticador na caixa **“Nome”**, ou marque a opção **“Automático”**;
- Insira o endereço IP do servidor onde está localizado o agente de autenticação. Por questões de segurança, o agente exige ainda a especificação de uma senha para que permita a comunicação de informações dos usuários e grupos que ele conhece. Deste modo, especifique a senha e a confirmação da mesma;
- Na caixa **“Domínios”**, insira o(s) domínio(s) local (is), ao(s) qual (is) o autenticador deverá estar relacionado. Este(s) domínio(s) já deve(m) estar referenciado(s) na Entidade **“Domínios”;**
- Em seguida, clique em **OK**.

Domínios

Nesta entidade podemos listar vários domínios que serão utilizados como base para diferentes filtros, tais como relay de e-mails permitido e bloqueio de remetentes.

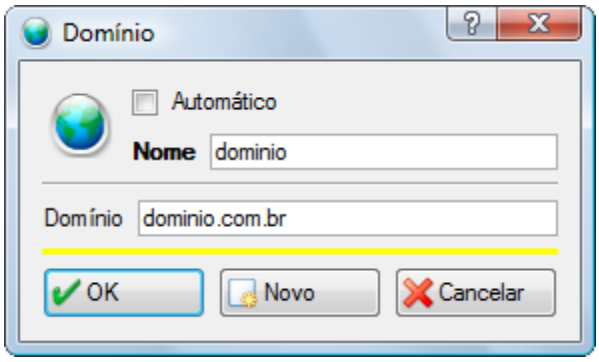

Figura 120. Configuração de entidades – domínio.

Para adicionar uma entidade do tipo “Domínio”:

- Clique com o botão direito do mouse sobre a entidade **“Domínio”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar a esta entidade no campo **“Nome”** ou marque a opção **“Automático”**;
- Informe o domínio desejado no campo designado e clique em **OK**;
- Para criar outras entidades do tipo “Domínio”, repita os passos quantas vezes forem necessárias.

Lista de Domínio

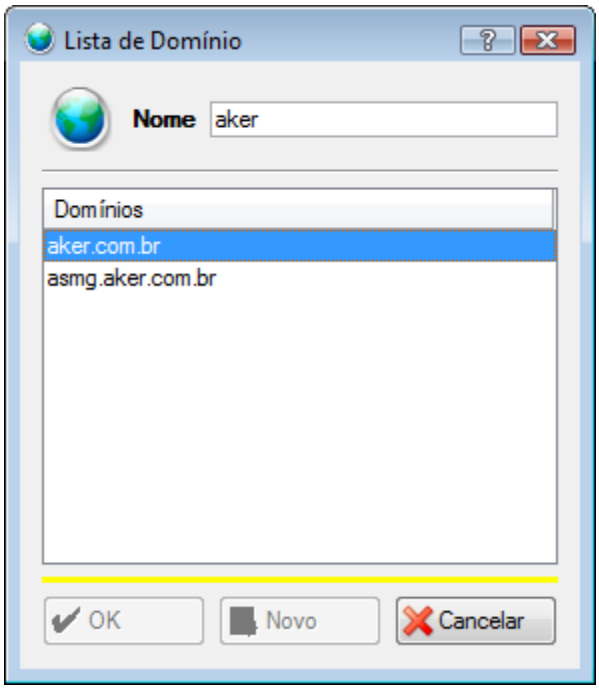

Figura 121. Configuração de entidades – lista de domínio.

Esta entidade é similar a entidade Domínio, porém permite em uma única entidade adicionar vários domínios facilitando a utilização nos filtros.

Para adicionar uma entidade do tipo “Lista de Domínio”:

- Clique com o botão direito do mouse sobre a entidade **“Lista de Domínio”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar a esta entidade no campo **“Nome”** ou marque a opção **“Automático”**;
- Na caixa **“Domínios”**, insira o(s) domínio(s)**.**
- Em seguida, clique em **OK**.

Para criar outras entidades do tipo “Lista de Domínio”, repita os passos quantas vezes forem necessárias.

Filtros Externos

É possível configurar programas ou scripts externos tais como antivírus ou analisadores de spams para, em conjunto com o **ASMG**, filtrar mensagens suspeitas ou mesmo contaminadas. O **ASMG** envia a mensagem para estes programas e, baseado na resposta dos mesmos, pode tomar atitudes diversas como, por exemplo, o descarte da mensagem.

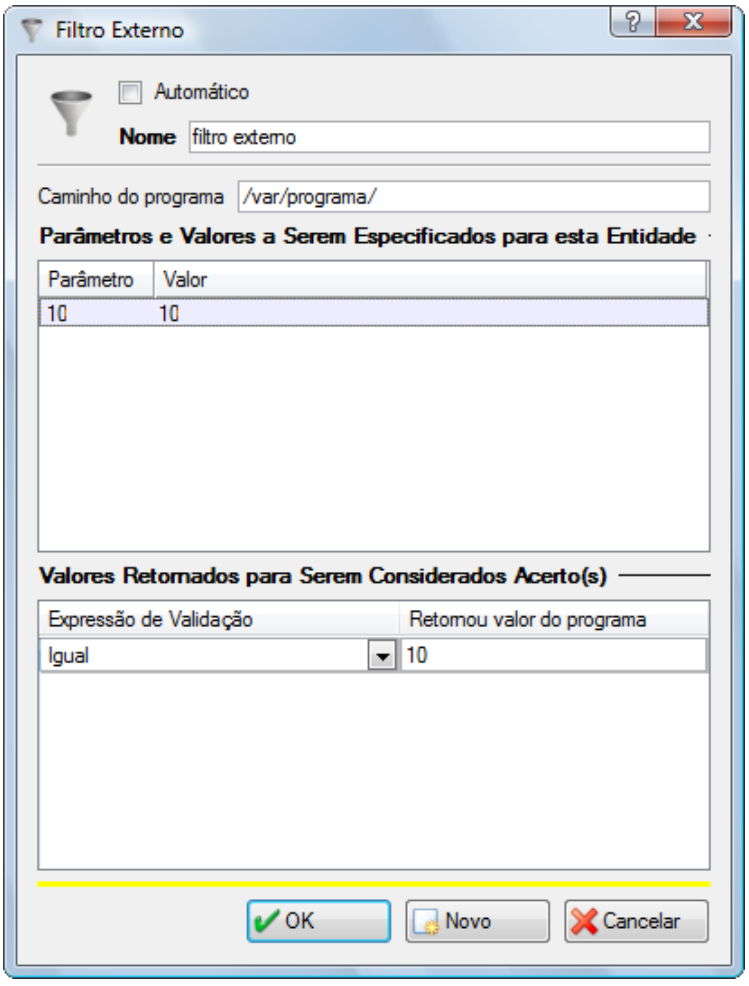

Figura 122. Filtro externo.

Para criar uma Entidade do tipo “Filtros Externos”:

- Clique com o botão direito do mouse sobre a entidade **“Filtros Externos”**;
- Selecione a opção **“Novo”**;
- Na tela seguinte, digite o nome que deseja dar ao filtro na caixa **“Nome”**, ou marque a opção **“Automático”**;
- Na caixa **“Caminho para o programa”**, informe o local correto onde o filtro externo pode ser encontrado (caminho para seu executável).

Também é possível especificar parâmetros e valores adicionais para serem utilizados pelos executáveis do programa escolhido e que, por sua vez, servirão como regras para a filtragem das mensagens. Para isso, siga os seguintes passos:

- Clique com o botão direito do mouse na tela **“Parâmetros e valores a serem especificados para esta Entidade”** e selecione **“Adicionar”**;
- Clique novamente o botão direito do mouse abaixo da coluna **“Parâmetro”** e adicione o parâmetro desejado. Se for o caso, repita este mesmo procedimento na coluna **“Valor”**;
- Para inserir novos parâmetros e valores, repita os passos 1 e 2 quantas vezes forem necessárias.

Vale ressaltar que para criar uma entidade deste tipo, é necessário que o administrador especifique pelo menos uma regra de valor retornado, pois é baseado neste valor de retorno que o **ASMG** decide o que vai fazer com a mensagem.

Lista de E-mails

Nesta entidade definimos listas de endereços eletrônicos que serão utilizados em diferentes situações dentro do **ASMG**.

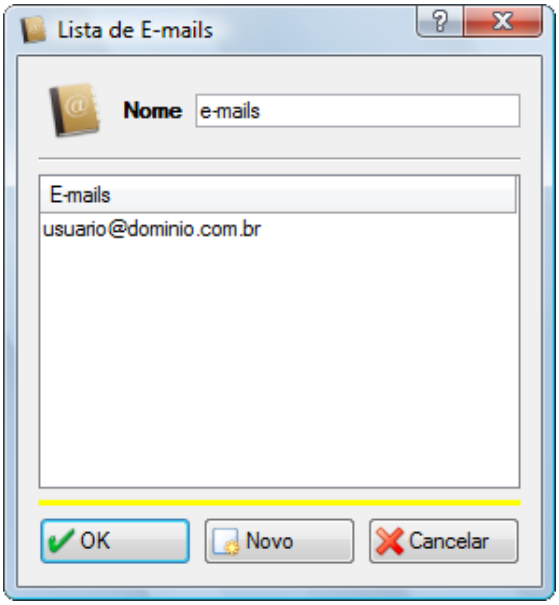

Figura 123. Lista de e-mails.

Para criar uma entidade do tipo “Lista de E-mails”:

- Clique com o botão direito do mouse sobre a entidade **“Listas de E-mails”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar à lista no campo **“Nome”**;
- Clique com o botão direito do mouse sobre a tela **“E-mails”** e clique em **“Novo”**;
- Digite o endereço desejado e clique em **OK**;
- Para inserir mais endereços na mesma lista, repita os passos 4 e 5, quantas vezes forem necessárias;
- Caso deseje criar mais de uma entidade do tipo **“Listas de E-mail”**, basta repetir os passos de 1 a 6, quantas vezes forem necessárias.

Há ainda a opção de importar as listas de endereços de e-mail diretamente de arquivos no formato **CSV**, ou exportá-las para arquivos neste mesmo formato. Para realizar a importação/exportação de uma lista:

- Clique com o botão direito do mouse sobre a entidade **“Listas de E-mails”**;
- Selecione a opção **“Novo”**;
- Selecione a opção **“Importar”** ou **“Exportar”**, conforme a ação desejada;
- Indique o nome do arquivo e o local onde ele está localizado. Clique em **“Importar”**, se estiver realizando uma importação, ou em **“Salvar”**, caso esteja exportando uma listas.

Listas de Expressões Regulares

Nesta entidade configuramos expressões mais sofisticadas a fim de identificarmos padrões de texto contidos em anexos das mensagens. Com elas, é possível identificar facilmente, por exemplo, se existe um anexo que faça referência a um endereço eletrônico, ou uma URL qualquer.

© Aker Security Solutions

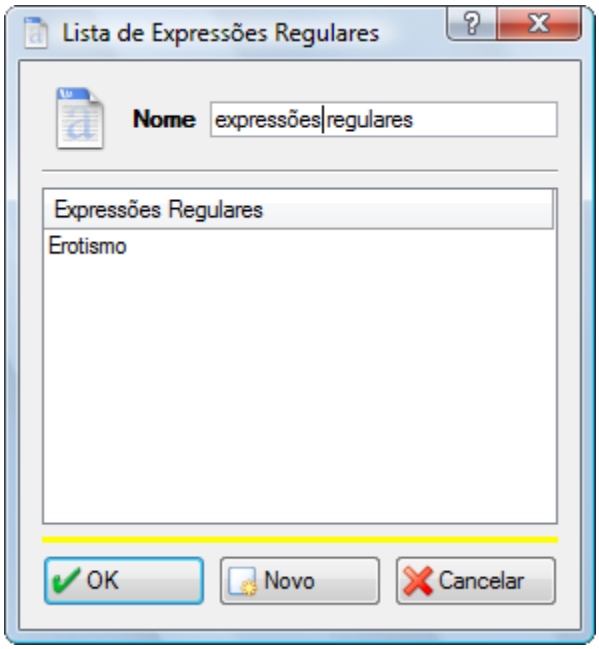

Figura 124. Lista de extressões regulares.

Apesar de ser um recurso bastante interessante, este tipo de filtragem possui uma análise mais complexa e que necessitam de consideráveis recursos computacionais. Assim, estas listas devem ser utilizadas com certa parcimônia.

Para criar uma entidade do tipo “Lista de Expressões Regulares”, proceda da seguinte maneira:

- Clique com o botão direito do mouse sobre a entidade **“Listas de Expressões Regulares”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar à lista no campo **“Nome”**;
- Clique com o botão direito do mouse sobre a tela **“Expressões Regulares”** e clique em **“Novo”**;
- Digite a expressão desejada e clique em **OK**;
- Para inserir mais expressões na mesma lista, repita os passos 4 e 5, quantas vezes forem necessárias;
- Caso deseje criar mais entidades do tipo “Listas de Expressões Regulares”, repita os passos quantas vezes forem necessárias.

É possível criar várias listas com expressões diferentes, agrupadas de maneira distinta. Se for este o caso, repita este procedimento quantas vezes forem necessárias.

Há ainda a opção de importar as listas de expressões regulares diretamente de arquivos no formato **CSV** ou exportá-las para arquivos neste mesmo formato. Para realizar a importação/exportação de uma lista:

- Clique com o botão direito do mouse sobre a entidade **"Listas de Expressões Regulares"**;
- Selecione a opção **"Novo"**;
- Selecione a opção **"Importar"** ou **"Exportar"**, conforme a ação desejada;
- Indique o nome do arquivo e o local onde ele está localizado. Clique em **"Importar"**, se estiver realizando uma importação, ou em **"Salvar"**, caso esteja exportando uma lista.

Não há restrições quanto à importação ou exportação de várias listas. Neste caso, basta repetir o procedimento acima.

As pesquisas usando expressões regulares são case-sensitive.

Listas de Palavras-Chave

Nesta entidade configuramos restrições para palavras-chave contidas em anexos do tipo texto das mensagens. Palavras-chave são entidades que representam listas de palavras tipicamente utilizadas em determinado assunto. Por exemplo: "vendas", "acesse", "site", são palavras tipicamente encontradas em anexos de mensagens de SPAM que fazem publicidade de produtos.

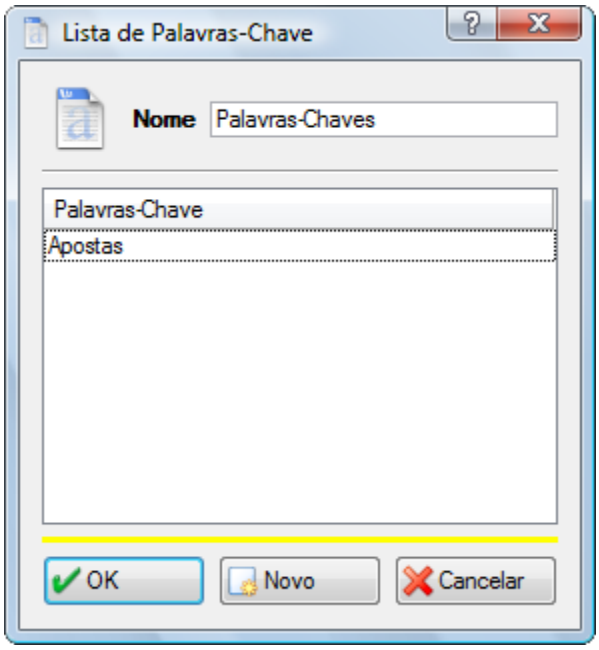

Figura 125. Lista de palavras-chave.

É possível criar várias listas com palavras-chaves diferentes, agrupadas, ou não, por determinado assunto. Para criar uma lista de palavras-chave, proceda da seguinte maneira:

- Clique com o botão direito do mouse sobre a entidade **"Listas de Palavras-Chave"**;
- Selecione a opção **"Novo"**;

- Na tela seguinte, digite o nome que deseja dar à lista no campo **"Nome"**;
- Clique com o botão direito do mouse sobre a tela **"Palavras-Chave"** e clique em **"Novo"**;
- Digite a palavra desejada e clique em **OK**;
- Para inserir mais Palavras-Chave dentro de uma mesma lista, repita os passos 4 e 5, quantas vezes forem necessárias;
- Caso deseje criar mais entidades do tipo "Listas de Palavras-Chave", repita os passos de 1 a 6, quantas vezes forem necessárias.

Há ainda a opção de importar as listas de palavras-chaves diretamente de arquivos no formato **CSV** ou exportá-las para arquivos neste mesmo formato. Para realizar a importação/exportação de uma lista:

- Clique com o botão direito do mouse sobre a entidade **"Listas de Palavras-Chave"**;
- Selecione a opção **"Novo"**;
- Selecione a opção **"Importar"** ou **"Exportar"**, conforme a ação desejada;
- Indique o nome do arquivo e o local onde ele está localizado. Clique em **"Importar"**, se estiver realizando uma importação, ou em **"Salvar"**, caso esteja exportando uma lista.

As pesquisas usando Palavras-Chave são case-sensitive.

RBLs

A entidade do tipo "RBL" referencia listas do tipo *Realtime Blackhole Lists*, que contêm endereços de servidores comumente utilizados para enviar mensagens de SPAM. Como estas listas são atualizadas constantemente e fazem a pesquisa *on-line*, convêm cadastrar os endereços de consulta para filtrar servidores promíscuos, entidades com as quais o **ASMG** não deseja se comunicar.

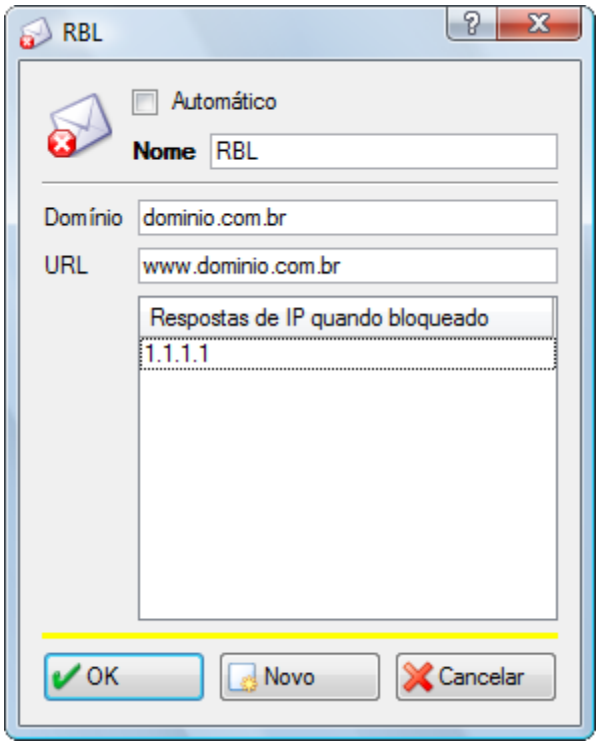

Figura 126. Entidade tipo RBL.

Por padrão, durante a instalação o **ASMG** já fornece um conjunto destas entidades pré-criadas representando as RBL's mais comuns. Mesmo assim, se o Administrador desejar configurar uma entidade do tipo “RBL”, basta seguir estes passos:

- Clique com o botão direito do mouse sobre a entidade **“RBLs”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar a esta entidade no campo **“Nome”** ou marque a opção **“Automático”**;
- Informe o domínio e a URL onde a lista está localizada;
- Para informar os IPs de resposta, clique com o botão direito do mouse sobre a tela **“Respostas de IP quando bloqueado”** e informe o IP de resposta, seguindo as orientações de configuração da RBL. Clique em **OK**.
- Para inserir outras RBLs, repita os passos quantas vezes forem necessárias.

Redes

Nesta entidade podemos configurar vários endereços de redes, tais como endereço do *gateway*, redes com *relay* permitido e também aquelas com conexão recusada, utilizados em filtros que serão configurados oportunamente.

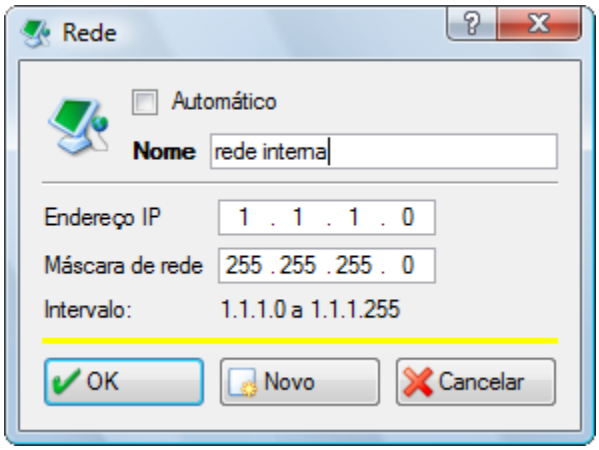

Figura 127. Entidade tipo Rede.

Para adicionar uma entidade do tipo “Rede”:

- Clique com o botão direito do mouse sobre a entidade **“Redes”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar a esta entidade no campo **“Nome”** ou marque a opção **“Automático”**;
- Informe o endereço IP e a máscara de rede nos campos designados e clique em **OK**;
- Para criar outras entidades do tipo “Redes”, repita os passos quantas vezes forem necessárias.

Servidores

Esta entidade representa os servidores internos ou externos a uma rede e que, para efeito de filtragem e/ou configuração, precisam ser referenciados no **ASMG**. Podemos citar como exemplos de utilização desta entidade a configuração do servidor interno de correio ou então a filtragem de servidores que tentem estabelecer conexões suspeitas.

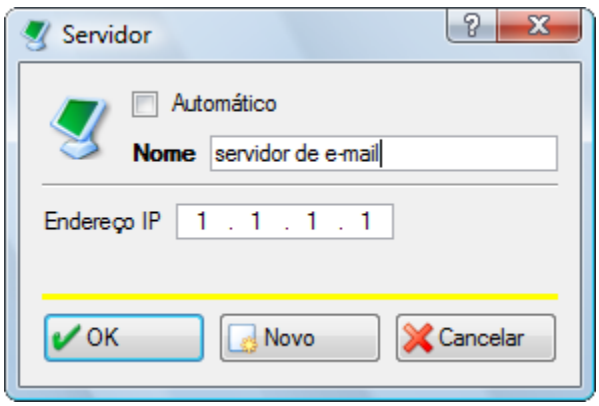

Figura 128. Entidade tipo Servidor.

Para adicionar uma entidade do tipo “Servidores”, faça o seguinte:

- Clique com o botão direito do mouse sobre a entidade **“Servidor”**;
- Selecione a opção **“Novo”**;
- Digite o nome que deseja dar a esta entidade no campo **“Nome”** ou marque a opção **“Automático”** caso não deseje adicionar nenhum;
- Informe o endereço IP do servidor no campo designado e clique em **OK**;
- Caso deseje criar mais entidades do tipo “Servidor”, repita os passos de 1 a 4, quantas vezes forem necessárias.

© Aker Security Solutions

Interface Gráfica do Usuário

17. Interface Gráfica do Usuário

A Interface Gráfica do Usuário é um modo de administração via web que pode ser habilitado pelo Administrador a fim de permitir que cada usuário possa personalizar suas opções, no que se refere ao recebimento de mensagens. Estas configurações incluem:

- Visualizar mensagens em quarentena de confirmação (caso esta funcionalidade esteja em uso);
- Visualizar mensagens em quarentena de filtros de e-mails;
- Criar listas de palavras-chave aceitas;
- Criação de *whitelist* pessoal;
- Criação de lista de bloqueio pessoal (*blacklist*);
- Opções gerais.

Para cada usuário é criado um arquivo no servidor, onde as informações pessoais são armazenadas. Quando uma mensagem chega, o **ASMG** verifica se o usuário possui configurações pessoais. Caso a resposta seja positiva, o sistema utiliza as listas criadas pelo usuário para em conjunto com as listas globais, filtrar as mensagens e decidir que ação deve ser tomada. Caso a resposta seja negativa, os filtros utilizados serão aqueles definidos pelas políticas.

A tela inicial de acesso à interface gráfica do usuário segue abaixo:

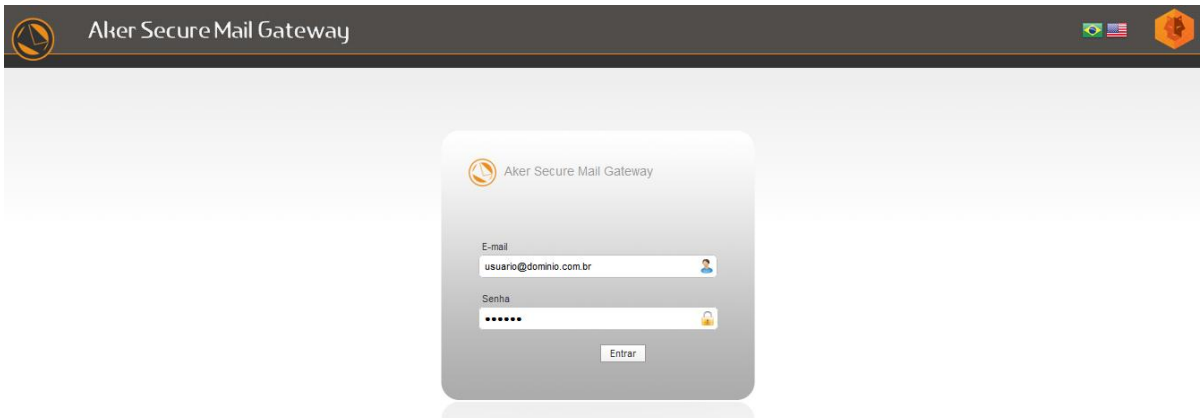

Figura 129. Tela de acesso inicial ao ASMG- interface gráfica.

Nesta tela, os usuários devem digitar seu login de rede, seguidos do domínio de rede. Note que, para o acesso à interface, deve ter sido previamente cadastrado na interface de administração uma entidade do tipo Autenticador, a qual tenha acesso à base de dados de usuários e grupos que se deseja utilizar. Além disso, é necessário que esta entidade esteja devidamente associada ao domínio de rede citado anteriormente.

© Aker Security Solutions

O endereço a ser fornecido pelo usuário ao navegador deve ser divulgado para os usuários da empresa. O caminho completo de acesso à interface é:

http://nome-da-maquina/webgui

Onde "nome-da-maquina" é o nome atribuído à máquina onde está instalado o ASMG.

Nas próximas seções explicaremos as funções de cada tela e as opções existentes em cada uma.

Quarentena de Confirmação

Nesta tela são apresentadas todas as mensagens que ainda aguardam a confirmação do remetente, e que possuam como destinatário o usuário que acessa a interface, caso a função **"Quarentena de Confirmação"** esteja ativa. Por padrão, a confirmação é habilitada automaticamente quando o usuário opta por utilizar a configuração pessoal.

Nesta tela, pode-se visualizar os campos **"Remetente"** e **"Assunto"** de cada mensagem, bem como classificar a relação de mensagens em ordem crescente ou decrescente, a partir do campo **"Assunto"**. Além disso, é possível realizar buscas, bastando para isso inserir a string no local indicado e clicar no botão **"Pesquisar"**.

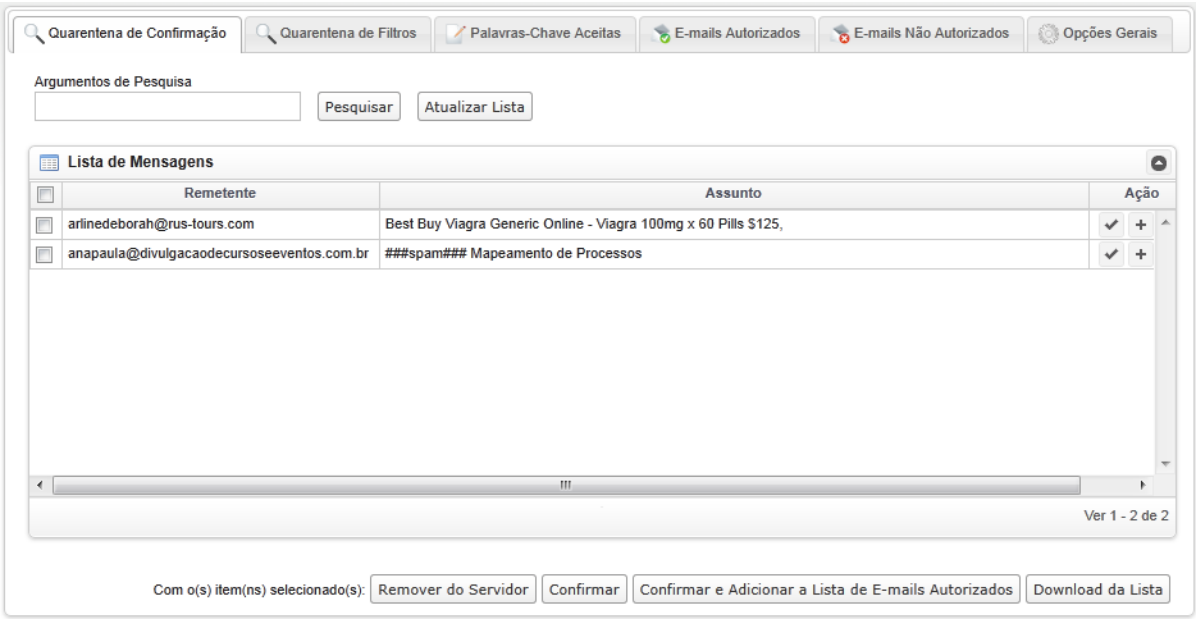

Figura 130. Quarentena de confirmação.

Como opção, pode-se selecionar determinadas mensagens e fazer com que elas sejam removidas do servidor, ou então confirmá-las automaticamente, fazendo com que sejam encaminhadas direto para a caixa de entrada do destinatário. É

importante frisar que, neste caso, o remetente não será adicionado à *whitelist* global e assim outra solicitação de confirmação será enviada quando este remetente enviar nova mensagem.

Quando aberta a tela de **"Quarentena de Confirmação",** o usuário terá acesso apenas à lista de mensagem. Para verificar se existem novas mensagens no servidor é necessário entrar o item **"Atualizar Pesquisa"**.

Para a **"Lista de Mensagens"** já cadastrada, é possível realizar as seguintes ações:

- Para remover do servidor a mensagem: basta selecionar na fleg a mensagem rementente a ser removida e clicar **"Remover do Servidor"**.
- Para confimação basta selecionar a fleg o remetente/mensagem e "Confirmar". A mesma será enviada ao destinatário.
- Para confirmar a permissão de recebimento e adicionar o remente a lista de e-mails autorizados, basta selecionar a fleg com a mensagem/destinatário desejado e clicar em **"Confirmar e Adicionar a lista de E-mails autorizados"**.
- Caso queira realizar um download da lista, basta clicar em **"Download da Lista",** irá aparecer à mensagem: **"Deseja salvar ou abrir este arquivo"**, basta clicar na opção desejada e a lista será aberta ou salva.

Quarentena de Filtros

Nesta tela são apresentadas todas as mensagens do usuário logado que foram bloqueadas por algum filtro do ASMG.

Aqui pode-se visualizar os campos: **"Remetente"** e **"Assunto"** de cada mensagem, bem como classificar a relação de mensagens em ordem crescente ou decrescente, a partir do campo **"Argumentos de Pesquisa"**. Além disso, é possível realizar buscas, basta para isso inserir a string no local indicado e clicar no botão **"Atualizar Lista"**.

© Aker Security Solutions

Figura 131. Quarentena de filtros.

Como opção, pode-se selecionar determinadas mensagens e fazer com que elas sejam removidas do servidor, ou então reenfileiradas, fazendo com que sejam encaminhadas direto para a caixa de entrada do destinatário.

Quando aberta a tela de **"Quarentena de Filtros",** o usuário terá acesso apenas à lista de mensagem. Para verificar se existem novas mesagens no servidor é necessário entrar o item **"Atualizar Pesquisa"**.

Para a **"Lista de Mensagens"** já cadastrada, é possível realizar as seguintes ações:

- Para remover do servidor a mensagem: basta selecionar na fleg a mensagem rementente a ser removida e clicar **"Remover do Servidor"**.
- Para reenfileirar mensangens basta selecionar a fleg o remetente/mensagem e clicar em **"Reenfileirar"**.
- Para reenfileirar e adicionar o remente a lista de e-mails autorizados, basta selecionar a fleg com a mensagem/destinatário desejado e clicar em **"Reenfileirar e Adicionar a Lista de E-mais Autoriazados"**.
- Caso queira realizar um download da lista, basta clicar em **"Download da Lista",** irá aparecer à mensagem: **"Deseja salvar ou abrir este arquivo"**, basta clicar na opção desejada e a lista será aberta ou salva.

© Aker Security Solutions

Palavras-Chave Aceitas

Nesta tela o usuário pode criar uma lista pessoal de palavras ou expressões que, se listadas no campo **"Palavras-chave/Frase"**, fará com que a mensagem seja repassada diretamente para a caixa de entrada do usuário, sem que seja necessário ao remetente confirmar seu envio.

Como aplicação interessante para esta tela, pode-se citar as listas de discussão na Internet, onde a confirmação de mensagens torna-se inviável. Assim, ao adicionar as strings ou assunto(s) do(s) grupo(s) a esta relação, a mensagem é repassada automaticamente para o destinatário.

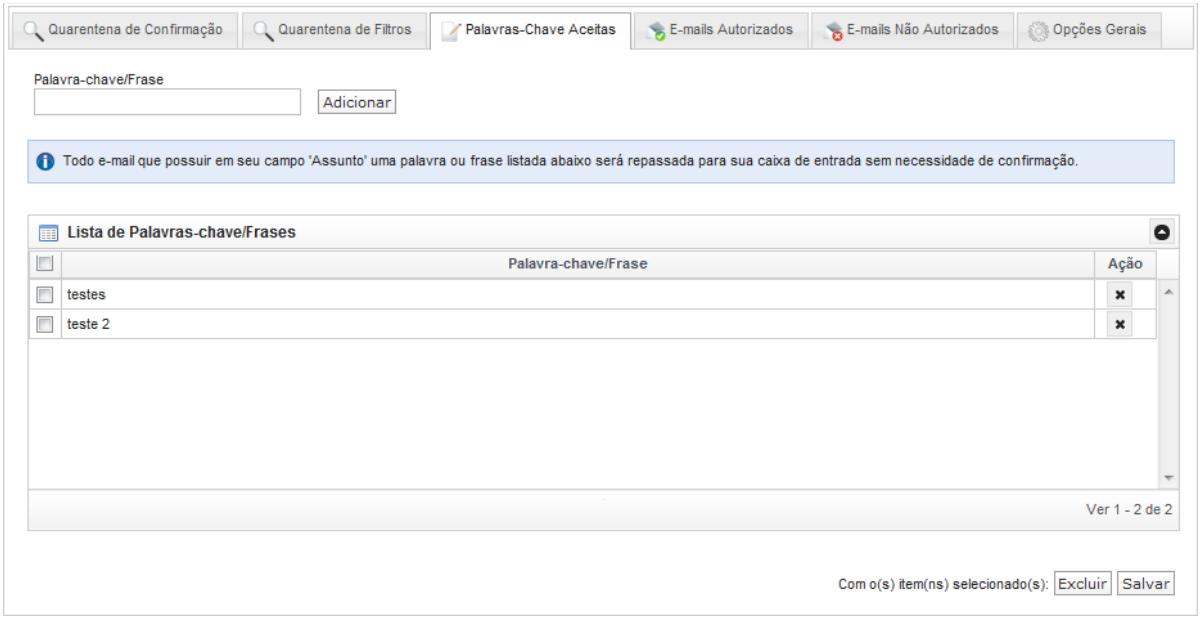

Figura 132. Palavras-chave aceitas.

E-mails Autorizados

Nesta tela o usuário pode incluir ou excluir endereços que terão suas mensagens prontamente recebidas, sem precisar passar por confirmação. A maior vantagem desta lista é que o usuário pode inserir nela alguns remetentes selecionados, criando sua *whitelist* particular.

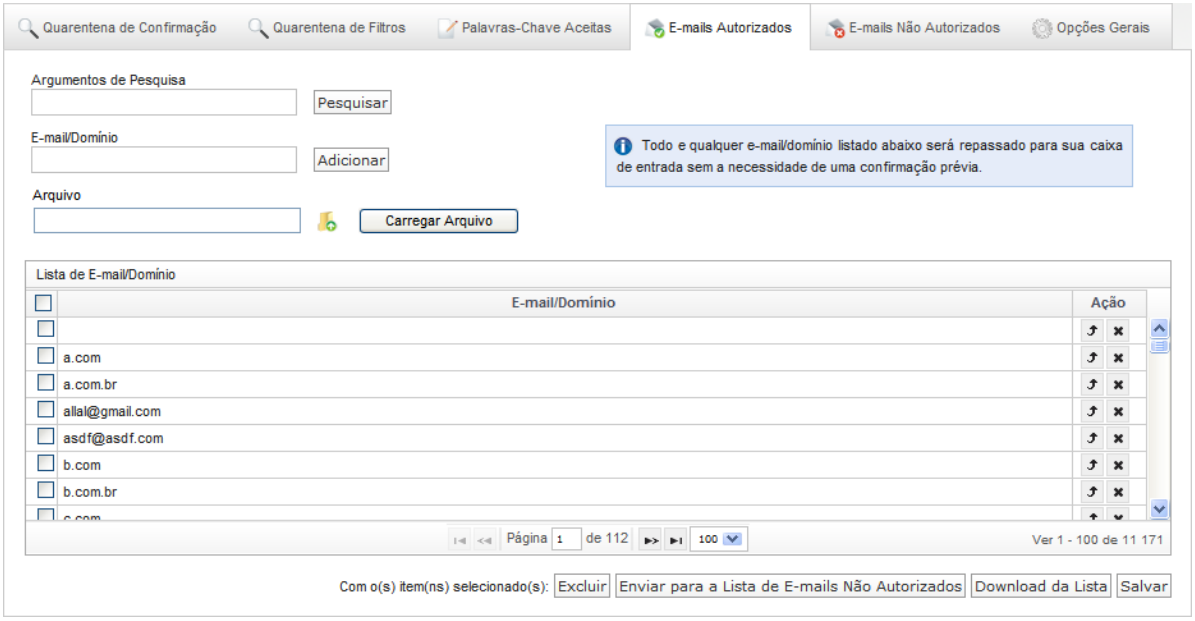

Figura 133. E-mails autorizados.

- Para realizar uma pesquisa, digitar o que deseja encontrar e clicar em **"Pesquisar"**;
- Para adicionar um domínio ou e-mail, digite na string o conteúdo desejado e em seguida, clicar em **"Adicionar"**;
- Para excluir mensagens, selecionar a fleg desejada e clicar em **"Excluir";**
- Caso queira enviar para lista de e-mails não autorizados, basta selecionar a fleg desejada e clicar em **"Enviar para a Lista de E-mails Não Autorizados";**
- Caso queira realizar um download da lista, basta clicar em **"Download da Lista",** irá aparecer à mensagem: **"Deseja salvar ou abrir este arquivo"**, basta clicar na opção desejada e a lista será aberta ou salva;
- Para salvar, clicar selecionar a fleg e clicar em **"Salvar"**.

Quando a mensagem chega, o **ASMG** verifica o endereço do remetente tanto na *whitelist* global como na pessoal. Caso encontre o remetente em uma das duas listas, a mensagem é entregue em seguida, sem precisar de confirmação por parte do remetente. Este tipo de configuração é interessante já que agiliza a entrega das mensagens.

É importante ressaltar que o fato de um endereço ser adicionado à lista particular de algum usuário não implica dizer que este mesmo endereço constará da lista global do **ASMG**. Se for este o caso, o remetente será orientado a confirmar a mensagem, caso envie alguma para outros usuários internos.

E-mails não Autorizados

Nesta tela, o usuário pode incluir ou excluir da relação, endereços que terão a permissão negada para envio de mensagens. Desta forma, caso um remetente possua seu endereço listado aqui, sua mensagem será automaticamente descartada e não chegará ao destino especificado, mesmo que o endereço esteja na *whitelist* global. Isto acontece porque a pesquisa é feita inicialmente nas *blacklists* (tanto global quanto pessoal) e, caso o endereço conste em algumas delas, a mensagem será recusada, durante a conexão entre os servidores.

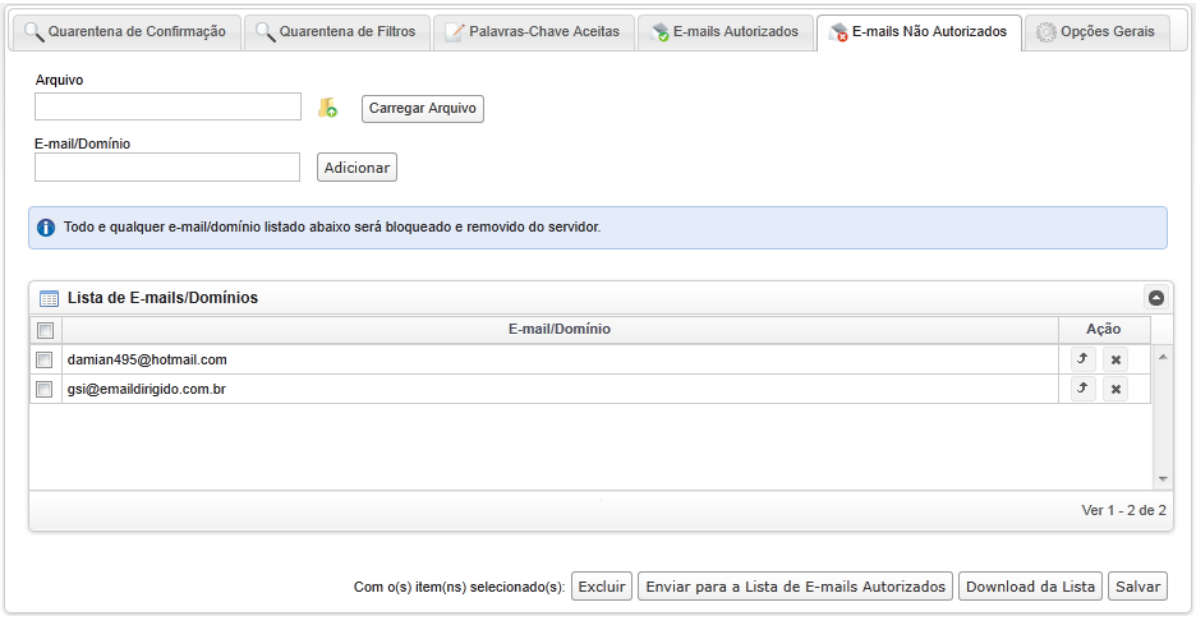

Figura 134. E-mails não autorizados.

Para as mensagens bloqueadas, o remetente recebe como resposta uma mensagem de erro, informando que a entrega não pôde ser realizada.

- Para encontrar um arquivo, digitar o que deseja na string e clicar em **"Carregar Arquivo"**;
- Para adicionar um domínio ou e-mail, digite na string o conteúdo desejado e em seguida, clicar em **"Adicionar"**;
- Para excluir mensagens, selecionar a fleg desejada e clicar em **"Excluir"**;
- Caso queira enviar para lista de e-mails autorizados, basta selecionar a fleg desejada e clicar em **"Enviar para a Lista de E-mails Autorizados";**
- Caso queira realizar um download da lista, basta clicar em **"Download da Lista",** irá aparecer à mensagem: **"Deseja salvar ou abrir este arquivo"**, basta clicar na opção desejada e a lista será aberta ou salva;
- Para salvar, clicar selecionar a fleg e clicar em **"Salvar"**.

© Aker Security Solutions

Opções Gerais

Nesta tela, o usuário personaliza as opções referentes ao comportamento do **ASMG** quando da recepção das mensagens.

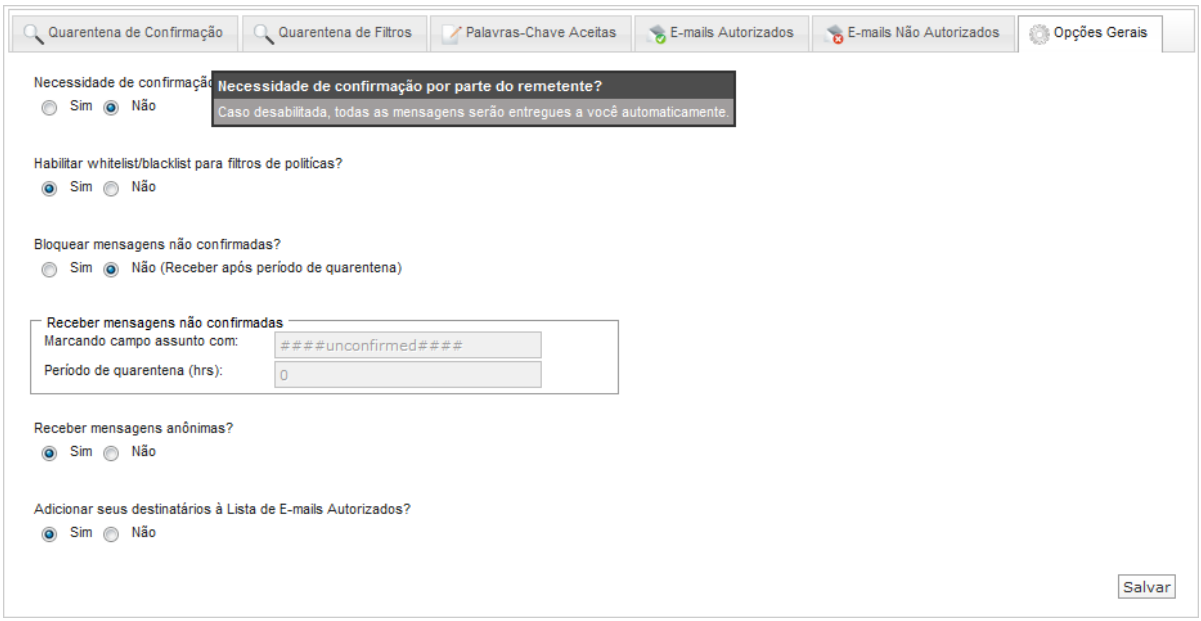

Figura 135. Opções gerais.

Dentre as opções disponíveis o usuário pode:

- Se na opção **"Necessidade de confirmação por parte do remetente?"** estiver selecionado o "Sim", todas as mensagens deverão ser confimadas pelo remente. Se estiver selecionado o **"Não",** todas as mensagens serão entregues automaticamente ao destinatário;
- Se na opção **"Habilitar whitelist/blacklist para filtros de políticas" estiver** selecionado o **"Sim"** todos os filtros serão utilizados e se estiver selecionado o **"Não"** nenhum filtro será utilizado;
- Se na opção **"Bloquear mensagens não confirmadas"** estiver selecionado o **"Sim"** todas as mensagens não confirmadas serão automaticamente bloqueadas. Caso seja selecionado o **"Não"** todas as mensagens não confirmadas serão enviadas aos destinatários;
- Se na opção **"Receber mensagens anônimas"** estiver selecionado o **"Sim"** todas as mensagens anônimas serão automaticamente recebidas. Caso seja selecionado o **"Não"** todas as mensagens anônimas não serão recebidas pelos destinatários;
- Se na opção **"Adicionar seus destinatários à Lista de E-mails Autorizados"** estiver selecionado o **"Sim"** todos os destinatários serão automaticamente adicionados na whitelist pessoal. Caso seja selecionado o **"Não"** todas os destinatários não serão adicionados;

Para concluir a configuração, deve-se clicar em **“Salvar”**.

É importante salientar que o fato da confirmação de mensagem estar desabilitado pode favorecer o recebimento de mensagens indevidas na caixa postal do usuário, já que neste caso não há controle quanto aos remetentes.

© Aker Security Solutions

Cluster

18. Cluster

Neste capítulo mostraremos como configurar a tolerância a falhas do ASMG.

Planejando a Instalação

O que é um sistema de tolerância às falhas?

Quanto mais os computadores ganham espaço nas empresas, nos escritórios e na vida das pessoas em geral, mais se ouve falar em "alta disponibilidade". Por um simples e bom motivo: nenhum usuário quer que a sua máquina pare de funcionar ou que os recursos de rede não possam mais ser acessados. É justamente a alta disponibilidade que vai garantir a continuidade de operação do sistema na prestação de serviços de rede, armazenamento ou processamento, mesmo se houver falhas em um ou mais de seus elementos.

Assim, alta disponibilidade é hoje um assunto que interessa a um número cada vez maior de usuários. Tornou-se um requisito fundamental para os sistemas que ficam no ar 24 horas por dia, sete dias por semana, ou que não possam ficar fora do ar por até mesmo alguns minutos. Afinal, paradas não planejadas podem comprometer, no mínimo, a qualidade do serviço, sem contar os prejuízos financeiros.

Tolerância às falhas nada mais é que um agrupamento de recursos que fornece ao sistema a ilusão de um recurso único. A maioria dos seus componentes encontra-se duplicados, desta forma, mesmo que um componente individual apresente falhas o serviço não é comprometido. Para possibilitar a redundância de recursos é necessário um mecanismo de gerência, de forma a tornar seu funcionamento transparente.

Como trabalha a Tolerância às Falhas do ASMG?

A tolerância às falhas do ASMG é composta por dois sistemas idênticos, ou seja, duas máquinas com o mesmo Sistema Operacional, mesmas placas de rede e com a mesma versão do produto, conectadas entre si. A exigência de se usar o mesmo sistema operacional se dá pelo fato de poder aplicar correções através da interface gráfica e essas correções serem replicadas automaticamente de uma máquina para a outra.

Além de estarem conectadas entre si, o que deve ser feito por uma interface de rede, é necessário que todas as placas de rede correspondentes das duas

máquinas estejam conectadas em um mesmo hub ou switch, de forma que ambas as máquinas tenham acesso às mesmas redes.

Configurando o Cluster do ASMG

As configurações do cluster do ASMG são efetuadas via linha de comando (Shell) nas duas máquinas de forma separadamente, abaixo segue as opções do comando “asmgcluster”:

```
# asmgcluster ajuda

asmgcluster - Ferramenta para configuração de cluster do ASMG

Uso: asmgcluster [ajuda | status | ativa | desativa]

    asmgcluster config <senha> <interface> <porta> <ip_virtual>

    asmgcluster local <hostname> <ip_real> [primario]

    asmgcluster remoto <hostname> <ip_real>


Ajuda:

    ajuda    = Mostra esta mensagem

    status   = Mostra a configuração atual do cluster

    ativa    = Ativa o funcionamento do cluster neste no'

    desativa = Desativa o funcionamento do cluster neste no'

            (Use -f para forçar desativação)

    config   = Configura os atributos gerais do cluster

            <senha>      = senha para reconhecimento do outro no'

            <interface> = interface de comunicação com o outro no'

            <porta>      = porta UDP de comunicação com o outro no'

            <ip_virtual> = Endereço IP do cluster quando ativo

    local    = Configura este no' do cluster
```

<hostname> = Nome deste no' no cluster

<ip_real> = Endereço IP que faz parte do cluster

primario = Este no' deve ser o primario

remoto = Configura as informações do no' remoto

<hostname> = Nome do no' remoto no cluster

<ip_real> = Endereço IP do no' remoto que faz parte do cluster

Mostrando configurações atuais

Sintaxe: asmgcluster status

Ação:

- Lê arquivos de configuração;
- Faz conversão dos dados para que sejam mostrados na tela.

Saída:

- Status do cluster (configurado, habilitado, etc.);
- Nós do cluster (IPs reais, hostnames, etc.);
- Senha (?);
- IP virtual do cluster;
- E-mail para notificação.

Habilitando cluster

Sintaxe: asmgcluster ativa

Ação:

- Valida configurações atuais;
- Atualiza configurações nos nós;
- Atualiza repositórios nos nós (partições);
- Inicia serviços necessários nos nós.

Saída:

- Mostrar mensagem de sucesso, com dados sobre nós possíveis;
- Ou mostrar mensagem de erro, se for o caso.

© Aker Security Solutions

Desabilitando cluster

Sintaxe: asmgcluster desativa

Ação:

- Desconfigura cluster nos nós;
- Atualiza configurações e repositórios nos nós;
- Pára serviços e desmonta partições.

Saída:

- Mostrar mensagem de sucesso ou erro.

Configurando nó primário do cluster

Sintaxe: asmgcluster local <hostname> <ip_address> primario

Ação:

- Salva configurações do ASMG;
- Se cluster habilitado, atualiza dados e reinicia serviços.

Saída:

- Mostrar mensagem de sucesso ou erro

Configurando nó secundário do cluster

Sintaxe: asmgcluster remoto <hostname> <ip_address>

Ação:

- Salva configurações do ASMG;
- Se cluster habilitado, atualiza dados e reinicia serviços.

Saída:

- Mostrar mensagem de sucesso ou erro

Configurando IP virtual e senha do cluster

Sintaxe: asmgcluster config <password> <interface do cluster> <porta de comunicação do cluster> <virtual_ip>

© Aker Security Solutions

Ação:

- Salva configurações do ASMG;
- Se cluster habilitado, atualiza dados e reinicia serviços.

Saída:

- Mostrar mensagem de sucesso ou erro

18..1. Exemplo de configuração

Topologia da rede

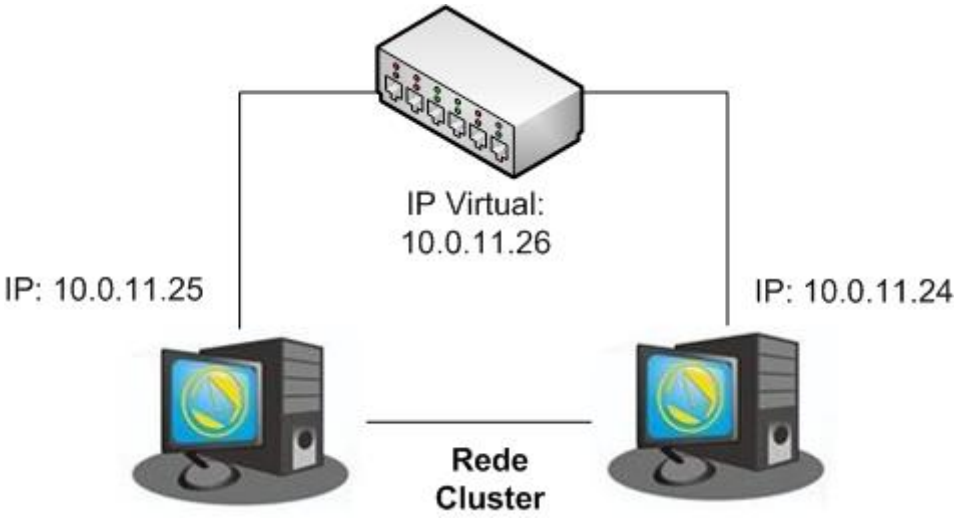

Figura 136. Exemplo de configuração – topologia da rede.

Configurando o ASMG Primário

Primeiro faça a configuração inicial com o comando "asmgcluster config <senha> <interface> <porta> <ip_virtual>" nos dois nós do cluster.

OBS: Rede do cluster é 192.168.0.0/30

Parâmetros:

senha: é a senha de autenticação entre os nós.

interface: é a interface utilizada na comunicação entre os nós.

porta: é a porta UDP que será utilizada na comunicação entre os nós.

ip_virtual: será o IP atribuído ao nó quando ele for o nó primário.

Após esta configuração, deve definir qual máquina será o nó primário e qual será o nó secundário, utilizando o comando "asmgcluster local <hostname> <ip_real> [primario]" com as informações do nó a ser configurado e "asmgcluster remoto <hostname> <ip_real>" com as informações do outro nó do cluster.

Parâmetros:

hostname: Nome da máquina.

ip_real: IP da máquina que será um dos nós do cluster.

primario: Parâmetro opcional que definirá qual nó será o nó primário.

Estes dois comandos devem ser executados nos dois nós do cluster, sendo que o nó primário será definido com o parâmetro "primario" no comando asmgcluster local.

Depois de configurado os dois nós do cluster, o comando "asmgcluster status" pode ser utilizado para verificar se os dados estão corretos e para saber em que estado o cluster se encontra. Caso as informações estejam incorretas, os comandos de configuração podem ser executados novamente para reconfigurar o cluster.

Após validar que as informações estão corretas, o cluster será ativado com o comando "asmgcluster ativa".

OBSERVAÇÃO: Este comando deve ser executado primeiro no nó primário e somente depois que o nó esteja ativado o comando deve ser executado no nó secundário.

Execute o comando "asmgcluster status" para saber o andamento da ativação.

Em nosso exemplo as configurações do Nó primário ficariam:

1. asmgcluster config 123456 eth1 1000 10.0.11.26
2. asmgcluster local asmg-node1.aker.com.br 192.168.0.1 primario
3. asmgcluster remoto asmg-node2.aker.com.br 192.168.0.2
4. asmgcluster ativa

© Aker Security Solutions

Após estes passos o ASMG irá construir uma nova partição no HD que será utilizada no cluster, isto pode demorar alguns minutos até algumas horas.

Configurando o ASMG Secundário

Segue a lista de comandos:

1. asmgcluster config 123456 eth1 1000 10.0.11.26
2. asmgcluster local asmg-node2.aker.com.br 192.168.0.2
3. asmgcluster remoto asmg-node1.aker.com.br 192.168.0.1
4. asmgcluster ativa

Após estes passos o ASMG irá construir uma nova partição no HD que será utilizada no cluster, isto pode demorar alguns minutos até algumas horas.

Verificando o status do Cluster

Através do comando “asmgcluster status”, podemos visualizar o status atual do cluster do ASMG, veja exemplo de quando está sendo efetuado um sincronismo entre as máquinas, esta situação ocorre quando reiniciamos uma das máquinas.

asmgcluster status

Configurações de cluster

Senha: 123456

Interface de controle: eth1

Porta UDP do Hearbeat: 1000

IP virtual: 10.0.11.26

Local: asmg-node1.aker.com.br 192.168.0.1

Remoto: asmg-node2.aker.com.br 192.168.0.2

No' local e' primario.

Status atual: Replicando...

Estado da conexão: SyncSource

No': Primario

Estado da partição: UpToDate

[=>.....] sincronizado: 14.0% (481932/555404)K

finaliza: 0:20:04 velocidade: 288 (316) K/sec.

Outro exemplo de quando está tudo sincronizado:

asmgcluster status

Configurações de cluster

Senha: 123456

Interface de controle: eth1

Porta UDP do Hearbeat: 1000

IP virtual: 10.0.11.26

Local: asmg-node1.aker.com.br 192.168.0.1

Remoto: asmg-node2.aker.com.br 192.168.0.2

No' local e' primario.

Status atual: Cluster ativado.

Estado da conexão: Connected

No': Primario

Estado da partição: UpToDate

Lista de Status do Cluster

Estado da conexão

- **StandAlone**: Sem configuração de rede disponível. Os outros nós não estão conectados ainda, ou foi desconectado administrativamente (usando drbdadm disconnect), ou dropou a conexão devida à falha de autenticação ou split brain.

- **Disconnecting**: Estado temporário durante a desconexão. O próximo estado é StandAlone.
- **Unconnected**: Estado temporário, anterior a uma tentativa de conexão. Próximos estados possíveis: WFConnection e WFReportParams.
- **Timeout**: Estado temporário seguido de um timeout na comunicação com o mestre. Próximo estado: Unconnected.
- **BrokenPipe**: Estado temporário depois que uma conexão com o mestre foi perdida. Próximo estado: Unconnected.
- **NetworkFailure**: Estado temporário depois que uma conexão com um nó foi perdida. Próximo estado: Unconnected.
- **ProtocolError**: Estado temporário depois que uma conexão com um nó foi perdida. Próximo estado: Unconnected.
- **TearDown**: Estado temporário. O mestre está fechando a conexão. Próximo estado: Unconnected.
- **WFConnection**: Este nó está esperando até que o nó mestre se torne visível na rede.
- **WFReportParams**: Conexão TCP foi estabilizada, este nó espera pelo primeiro pacote de rede do master.
- **Connected**: Uma conexão DRBD foi estabilizada, dados de espelhamento ativo. Este é o estado normal.
- **StartingSyncS**: Sincronização total, iniciada pelo administrador, começando. Os próximos estados possíveis são: SyncSource ou PausedSyncS.
- **StartingSyncT**:Sincronização total, iniciada pelo administrador, começando. Próximo estado: WFSyncUUID.
- **WFBitMapS**: Sincronização parcial começando. Próximos estados possíveis: SyncSource ou PausedSyncS.
- **WFBitMapT**: Sincronização parcial começando. Próximo estado: WFSyncUUID.
- **WFSyncUUID**: Sincronização está prestes a começar. Próximos estados possíveis: SyncTarget or PausedSyncT.
- **SyncSource**: Sincronização rodando, com o nó local sendo a fonte da sincronização.
- **SyncTarget**: Sincronização rodando, com o nó local sendo o destino da sincronização.
- **PausedSyncS**: O nó local é a fonte da sincronização em andamento, mas a sincronização está atualmente pausada. Isto pode ser causado devido a alguma dependência na finalização de outro processo de sincronização, ou devido à sincronização ter sido manualmente interrompida pelo drbdadm pause-sync.
- **PausedSyncT**: O nó local é o destino da sincronização em andamento, mas a sincronização está atualmente pausada. Isto pode ser causado devido a alguma dependência na finalização de outro processo de sincronização, ou

devido à sincronização ter sido manualmente interrompida pelo drbdadm pause-sync.

- **VerifyS**: Verificação de dispositivo on-line rodando, com o nó local sendo a fonte da verificação.
- **VerifyT**: Verificação de dispositivo on-line rodando, com o nó local sendo o destino da verificação.

Estado da partição

- **Diskless**: Nenhum bloco local do dispositivo foi assinado pelo driver DRBD. Isto pode significar que a fonte nunca foi ligada a este dispositivo de apoio, também pode ter sido manualmente desligado usando drbd detach ou foi desligado automaticamente depois de um erro de E/S de baixo nível.
- **Attaching**: Estado transitório enquanto os meta dados estão sendo lidos.
- **Failed**: Estado transitório seguido de uma falha de E/S reportada pelo bloco do dispositivo local. Próximo estado: Diskless.
- **Negotiating**: Estado transitório quando foi vinculado um dispositivo DRBD já conectado.
- **Inconsistent**: Os dados são inconsistentes. Este estado ocorre imediatamente após a criação de uma nova fonte, nos dois nós (antes da sincronização total inicial). Também, este estado pode ser encontrado em um nó (O destino da sincronização) durante a sincronização.
- **Outdated**: Os dados da fonte estão consistentes, mas desatualizados.
- **DUnknown**. Este estado é usado por um disco master se não tiver conexão de rede ativa. Consistent. Dados consistentes de um nó sem conexão. Quando a conexão é estabilizada, é decidido quais dados são atualizados ou desatualizados.
- **UpToDate**: Consistente, estado atualizado dos dados. Este é o estado normal.